APRIL 1900

ANNALS OF MATHEMATICS

(FOUNDED BY ORMOND STONE)

EDITED BY

ORMOND STONE W. E. BYERLY H. S. WHITE

W. F. OSGOOD MAXIME BÔCHER

PUBLISHED UNDER THE AUSPICES OF HARVARD UNIVERSITY

SECOND SERIES Vol. 1 No. 3

ALL COMMUNICATIONS should be addressed to *The Annals of Mathematics*,
2 University Hall, Cambridge, Mass.

Entered at the Post Office as second-class mail matter

RATIONAL TRIANGLES.

By Derrick N. Lehmer.

We wish in this paper to develop in a new way the theory of the general triangle, the sides and area of which are expressible in rational numbers: in particular we shall be chiefly concerned with triangles whose sides and area are expressible in integers. The method we shall employ will bring to light new properties of these triangles and at the same time will give a deeper insight into formulæ and theorems already well known.

A triangle with integral sides and area we will call an *integral triangle* and if the three numbers representing the sides have unity for their greatest common divisor, the triangle will be called a *reduced integral triangle*.

We start from the following well-known theorem:

Theorem I. *The sides a, b and hypotenuse c of any integral right triangle satisfy the proportion:*

$$a : b : c = 2a\beta : \alpha^2 - \beta^2 : \alpha^2 + \beta^2,$$

where α, β *are integers;* $\alpha > \beta > 0$.

To prove this,* we observe that we may write the hypotenuse c equal to $b + \beta/\alpha\, a$ where β/α is some proper fraction. We thus obtain:

$$a^2 + b^2 = c^2 = b^2 + 2ab\frac{\beta}{\alpha} + a^2\frac{\beta^2}{\alpha^2},$$

whence we derive at once:

$$\frac{b}{a} = \frac{\alpha^2 - \beta^2}{2\alpha\beta}.$$

Also since

$$\frac{c^2}{a^2} = 1 + \frac{b^2}{a^2},$$

* This proof of the theorem is to be found in Euler *Com. Arith.* Vol. I, p. 24–25. The following more general theorem was proved by Frenicle (*Traité des triangles rectangles en nombres.* Paris 1676 § § xxiv, xxv, pp. 59–61). *Any integral right triangle, the greatest common divisor of whose sides is a square or twice a square is given by integer values of* α, β *in the formulæ*

$$a = 2\alpha\beta,$$
$$b = \alpha^2 - \beta^2,$$
$$c = \alpha^2 + \beta^2,$$

and conversely.

we get:

$$\frac{c}{a}=\frac{\alpha^2+\beta^2}{2\alpha\beta}.$$

An angle whose sine and cosine are both rational, we will call a *rational angle*. It is clear that such an angle A, if we assume it less than 180°, will be an internal or external angle of an integral right triangle, and therefore by Theorem I:

$$\sin A=\frac{2\alpha\beta}{\alpha^2+\beta^2},$$

$$\cos A=\pm\frac{\alpha^2-\beta^2}{\alpha^2+\beta^2}.$$

THEOREM II. *If A and B are rational angles so also is $A\pm B$.*

This appears by expanding $\sin(A\pm B)$ and $\cos(A\pm B)$. It follows from this theorem that if two angles of a triangle are rational, so also is the third.

THEOREM III. *An integral triangle has rational angles; and conversely a triangle with rational angles is either an integral triangle or similar to one.*

For let the sides be a, b, c and the area K. From the relations:

$$\sin A=\frac{2K}{bc},$$

$$\cos A=\frac{b^2+c^2-a^2}{2bc},$$

we see that for integer values of a, b, c, and K the angle A is rational.

To prove the converse we may assume one side rational. For we may divide through by any side and get one side unity without disturbing the angles. Let a be rational. Then

$$b=a\frac{\sin B}{\sin A},$$

which is rational if the angles are. Similarly for c. Also

$$K=\tfrac{1}{2}\,bc\sin A$$

which is rational. Multiplying up by the least common denominator of a, b, c, and K the theorem follows.

It follows from this theorem that we may represent the sines and cosines

of the angles of an integral triangle by the following formulæ; taking C as the largest angle and therefore the only one whose cosine can be negative:

$$\sin A = \frac{2\alpha\beta}{\alpha^2+\beta^2}, \qquad \cos A = \frac{\alpha^2-\beta^2}{\alpha^2+\beta^2},$$

$$\sin B = \frac{2(\alpha\delta\pm\beta\gamma)(\alpha\gamma\mp\beta\delta)}{(\alpha^2+\beta^2)(\gamma^2+\delta^2)}, \quad \cos B = \frac{(\alpha\delta\pm\beta\gamma)^2-(\alpha\gamma\mp\beta\delta)^2}{(\alpha^2+\beta^2)(\gamma^2+\delta^2)},$$

$$\sin C = \frac{2\gamma\delta}{\gamma^2+\delta^2}, \qquad \cos C = \pm\frac{\gamma^2-\delta^2}{\gamma^2+\delta^2},$$

where $\alpha > \beta$, $\gamma \geqq \delta$.

From the fact that the sides of any triangle are proportional to the sines of the opposite angles we get the theorem:

THEOREM IV. *The formulæ*

$$a = \alpha\,\beta\,(\gamma^2+\delta^2),$$
$$b = (\alpha\,\delta \pm \beta\,\gamma)\;(\alpha\,\gamma \mp \beta\,\delta),$$
$$c = \gamma\,\delta\;(\alpha^2+\beta^2),$$

give the sides of integral triangles for integer values of $\alpha, \beta, \gamma, \delta$. *Conversely by the above formulæ an integral triangle may be found similar to any given one.**

We might have taken

$$\sin A = \frac{\alpha^2-\beta^2}{\alpha^2+\beta^2}, \qquad \cos A = \pm\frac{2\alpha\beta}{\alpha^2+\beta^2};$$

with similar variations for the other angles. We should thus have obtained formulæ apparently different from the above, but easily thrown into the same form.

---

* This theorem and the one following are given by Mr. Blichfeldt in the ANNALS OF MATHEMATICS, 1st Series, Vol. 11, p. 57. He derives the above formulæ in a very different way,—a way which gives him no hint of the geometrical meaning of the parameters $\alpha, \beta, \gamma, \delta$. The formulæ of this theorem seem to have been familiar to Euler (*Commentationes Arithmeticæ* Vol. II, p. 648) who gives them in the form

$$a : b : c = \frac{\gamma^2+\delta^2}{\gamma\delta} : \frac{(\alpha\delta\pm\beta\gamma)(\alpha\gamma\mp\beta\delta)}{\alpha\beta\gamma\delta} : \frac{\alpha^2+\beta^2}{\alpha\beta}.$$

Euler's method of obtaining them is not given; the article being a fragment of which the first twenty-six paragraphs are missing. The following theorem is also contained by implication in paragraph 33 of the same fragment.

THEOREM V. *In a reduced integral triangle the common factor of any two sides is the sum of two squares.*

This appears from the formula

$$a^2 = b^2 + c^2 - 2bc\frac{\alpha^2 - \beta^2}{\alpha^2 + \beta^2}.$$

For in a reduced triangle α and β must be taken relative primes. If then θ divides b and c it will also divide a unless it divides $\alpha^2 + \beta^2$. But the divisors of $\alpha^2 + \beta^2$ are all the sum of two squares. (*Cf.* Dirichlet Dedekind *Zahlentheorie*, p. 164.)

THEOREM VI. *The area of the triangle given by the above formulæ is:*

$$K = \alpha\beta\gamma\delta\,(\alpha\delta \pm \beta\gamma)\,(\alpha\gamma \mp \beta\delta).$$

THEOREM VII. *The radius of the circle circumscribed about the triangle given by the above formulæ is:*

$$R = \tfrac{1}{4}\,(\alpha^2 + \beta^2)\,(\gamma^2 + \delta^2).$$

It follows from the last theorem that in a reduced triangle the odd primes in $4R$ are all of the form $4n + 1$.

Also, from the proof of Theorem V, it follows that every divisor of two sides of such a triangle appears as a factor in four times the radius of the circumscribed circle.

THEOREM VIII. *If we fix α and β, and let γ and δ vary, the resulting triangles will all contain the angle A or its supplement.*

THEOREM IX. *For any particular values of the parameters α, β, γ, δ, we get two triangles inscribed in the same circle.*

For in both the triangles of Theorem IV

$$R = \tfrac{1}{4}\,(\alpha^2 + \beta^2)\,(\gamma^2 + \delta^2).$$

We may therefore superpose the circle circumscribing one triangle upon the circle circumscribing the other.

The two triangles are also seen to be such that two sides of one are equal respectively to two sides of the other.

THEOREM X. *The two triangles of the preceding theorem may be placed in the same circle, so that a side of one shall coincide with an equal side of the other. The extremities of this common side together with the two opposite vertices furnish the vertices of an inscribed quadrilateral with rational sides, area*

and diagonals. By producing opposite sides of this quadrilateral till they meet we get a cluster of six rational triangles. Further, the triangles formed by joining the vertices of the quadrilateral to the centre of the circle are also rational. Finally by proper multiplication we have all the lines and areas integral.

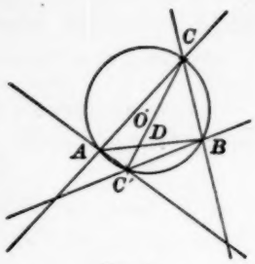


FIG. 1.

To prove this theorem let AB be the common side and let the two integral triangles be ABC and ABC'. Then the angle $BCC' = BAC'$ is rational. Also the angle CBC' is rational being the sum of two rational angles. Then the triangle CBC' has two rational angles and is therefore rational. The diagonal CC' is therefore rational. Also the angles of BDC' are rational so that BD is rational. Similarly for all the other lines of the figure.

COB is also a rational triangle having all its sides rational and the angle at O twice the rational angle CAB.

THEOREM XI. *A circle of rational radius may be found in which may be inscribed any specified number of integral triangles.*

Choose a number m which is made up of k distinct primes all of the form $4n+1$. We can then obtain 2^{k-1} different solutions of the indeterminate equation

$$\gamma^2 + \delta^2 = m.$$

(*Cf.* Dirichlet Dedekind *Zahlentheorie*, p. 164.) Give now α and β any fixed values. For every solution of the above equation we can construct two triangles whose circumscribed circles have a radius

$$\tfrac{1}{4}m\ (\alpha^2 + \beta^2).$$

By choosing k at will the theorem follows.

THEOREM XII. *We may cut up any rational triangle into an indefinite number of rational triangles.*

Let ABC be a rational triangle. Since an equilateral triangle is not rational, one angle A must be less than one other, say B. Lay off BD making the angle DBC equal to the angle A. The triangle BCD has two rational angles and one rational side, and is therefore rational. The same reasoning applies to the triangle ABD. The same process may be applied to these two rational triangles and so on sequentially.

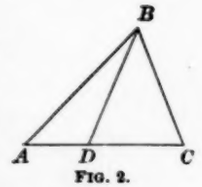


FIG. 2.

Kummer* has developed formulæ for quadrilaterals with rational sides, areas, and diagonals. Such a quadrilateral is divided by its diagonals into rational triangles, and the diagonals make with each other a rational angle. These facts might be of service in deriving formulæ for such quadrilaterals.

UNIVERSITY OF CHICAGO, JANUARY, 1900.

* Kummer: Ueber die Vierecke deren Seiten und Diagonalen rational sind. *Crelle*: Vol. 37, p. 1–20.

TWO ELEMENTARY GEOMETRICAL APPLICATIONS OF DETERMINANTS.

By H. S. White.

In attacking a geometrical problem by analytical methods we often have two courses open to us.

1. We may endeavor to simplify the problem as far as possible by a special choice of the coordinate system. This is deservedly a favorite method, but it usually involves a loss of symmetry which may overbalance the simplification. It not infrequently has the further disadvantage of making necessary a separate consideration of exceptional cases, a distinction irrelevant to the main problem having been introduced by the special coordinate system.

2. We may attempt to give to the analytical work the utmost possible symmetry. This method often calls for skill in the manipulation of algebraical expressions, and, in particular, readiness in the use of determinants.

A student who goes beyond the elements of geometrical study will soon find himself obliged to make use of the second of these methods, *e. g.* in the study of line geometry in three dimensions. It is well for him therefore to have practice in this kind of work, even in the solution of elementary problems where the first method is ordinarily used. With this idea in mind, the following symmetrical treatment of Desargues' and Pascal's theorems has been prepared. Incidentally attention is called (§ 3) to a rarely noticed natural connection between these theorems, the two sets of alternate sides of an inscribed hexagon constituting two triangles in perspective position, whose vertices suggest at once Brianchon's hexagon.

1. Notation and a Reducing Formula. Let a point be denoted by homogeneous coordinates, as x_1, x_2, x_3; a line by u_1, u_2, u_3; the triangle of reference being the same for both systems, and the two systems so chosen that when the line contains the point the equation is satisfied:

$$u_1 x_1 + u_2 x_2 + u_3 x_3 = 0.$$

If two points (p_1, p_2, p_3) and (q_1, q_2, q_3) lie on a line (u_1, u_2, u_3), the two equations yield the proportions: $u_1 : u_2 : u_3 = (p_2 q_3) : (p_3 q_1) : (p_1 q_2)$. Denote these two-rowed determinants by $(p\,q)_1$, $(p\,q)_2$, $(p\,q)_3$ respectively.

Similarly if two lines (u_1, u_2, u_3) and (v_1, v_2, v_3) determine a point (x_1, x_2, x_3), we find the proportions:

$$x_1 : x_2 : x_3 = (u_2 v_3) : (u_3 v_1) : (u_1 v_2) = (u\,v)_1 : (u\,v)_2 : (u\,v)_3.$$

Accordingly if two points (a) and (b) determine a line (u), and two others, (c) and (d), the line (v), while (u) and (v) meet in a point (x), there will be no obscurity in the following abbreviation:

$$\begin{aligned} x_1 : x_2 : x_3 \quad &= (u\,v)_1 : (u\,v)_2 : (u\,v)_3 \\ &= ((a\,b)_2\,(c\,d)_3) : ((a\,b)_3\,(c\,d)_1) : ((a\,b)_1\,(c\,d)_2) \\ &= (a\,b,\, c\,d)_1 : (a\,b,\, c\,d)_2 : (a\,b,\, cd)_3. \end{aligned}$$

For a particular example, suppose that the points (a) and (c) coincide, so that the point (x) is the point (a). This is shown from the above proportions by substituting for c_1, c_2, c_3 respectively a_1, a_2, a_3, so that we have

$$x_1 : x_2 : x_3 = [(a\,b)_2\,(a\,d)_3] : [(a\,b)_3\,(a\,d)_1] : [(a\,b)_1\,(a\,d)_2],$$

and then noticing that these are, save for sign, first minors of the determinant

$$D' = \begin{vmatrix} (ba)_1 & (ba)_2 & (ba)_3 \\ (ad)_1 & (ad)_2 & (ad)_3 \\ (db)_1 & (db)_2 & (db)_3 \end{vmatrix},$$

which is the conjugate or "reciprocal" of the determinant:

$$D = \begin{vmatrix} d_1 & d_2 & d_3 \\ b_1 & b_2 & b_3 \\ a_1 & a_2 & a_3 \end{vmatrix}.$$

Accordingly these minors are proportional to their complementary constituents in D, and are respectively equal to the following:

$$D \cdot a_1, \quad D \cdot a_2, \quad D \cdot a_3.$$

It will be necessary to reduce to simpler form several determinants whose constituents are themselves two-rowed determinants, like the following:

$$R = \begin{vmatrix} (ab)_1 & (cd)_1 & (xy)_1 \\ (ab)_2 & (cd)_2 & (xy)_2 \\ (ab)_3 & (cd)_3 & (xy)_3 \end{vmatrix}.$$

This may be expanded by distributing — so to term it — the constituents

of any one column. To distribute the third column, assume any arbitrary quantities z_1, z_2, z_3, and multiply R by the determinant $(x\,y\,z)$, column-wise:

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} \cdot R = \begin{vmatrix} (abx) & (cdx) & (xyx) \\ (aby) & (cdy) & (xyy) \\ (abz) & (cdz) & (xyz) \end{vmatrix}$$

$$= \begin{vmatrix} (abx) & (cdx) \\ (aby) & (cdy) \end{vmatrix} \cdot (xyz).$$

For (xyx) and (xyy) are identically zero. Omitting the factor (xyz) on each side of the above equation, we have the reduction desired:

$$R \equiv \Big((a\,b)_1 \;\; (c\,d)_2 \;\; (x\,y)_3 \Big) = (a\,b\,x) \;\; (c\,d\,y) - (a\,b\,y) \;\; (c\,d\,x).$$

Of course also the first or the second column could have been distributed, giving the alternative reductions:

$$\begin{aligned} R &= (a\,c\,d) \;\; (b\,x\,y) - (b\,c\,d) \;\; (a\,x\,y) \\ &= (a\,b\,d) \;\; (c\,x\,y) - (a\,b\,c) \;\; (d\,x\,y). \end{aligned}$$

2. Two perspective triangles,—Desargues' Theorem.

If two triangles $A\,B\,C$ and $D\,E\,F$ are so situated that lines joining corresponding vertices $A\,D$, $B\,E$, $C\,F$ meet in a point, then pairs of corresponding sides meet in three points of a right line.

The proof will be made by examining the condition $P=0$ for three lines meeting in a point, and the condition $L=0$ for three points lying on a line, and showing that P is a factor of L. Denoting the coordinates of A by a_1, a_2, a_3, etc., we have these two conditions in a form to which the reduction in §1 can be applied, as follows:

$$P = \begin{vmatrix} (ad)_1 \;\; (be)_1 \;\; (cf)_1 \\ (ad)_2 \;\; (be)_2 \;\; (cf)_2 \\ (ad)_3 \;\; (be)_3 \;\; (cf)_3 \end{vmatrix} = (ade)(bcf) - (adb)(ecf);$$

$$L = \begin{vmatrix} (ab,\, de)_1 \;\; (bc,\, ef)_1 \;\; (ca,\, fd)_1 \\ (ab,\, de)_2 \;\; (bc,\, ef)_2 \;\; (ca,\, fd)_2 \\ (ab,\, de)_3 \;\; (bc,\, ef)_3 \;\; (ca,\, fd)_3 \end{vmatrix}$$

$$= \begin{vmatrix} (ab)_1 & (de)_1 & (ca)_1 \\ (ab)_2 & (de)_2 & (ca)_2 \\ (ab)_3 & (de)_3 & (ca)_3 \end{vmatrix} \cdot \begin{vmatrix} (bc)_1 & (ef)_1 & (fd)_1 \\ (bc)_2 & (ef)_2 & (fd)_2 \\ (bc)_3 & (ef)_3 & (fd)_3 \end{vmatrix}$$

$$- \begin{vmatrix} (ab)_1 & (de)_1 & (fd)_1 \\ (ab)_2 & (de)_2 & (fd)_2 \\ (ab)_3 & (de)_3 & (fd)_3 \end{vmatrix} \cdot \begin{vmatrix} (bc)_1 & (ef)_1 & (ca)_1 \\ (bc)_2 & (ef)_2 & (ca)_2 \\ (bc)_3 & (ef)_3 & (ca)_3 \end{vmatrix}.$$

Reducing this still further, we find:

$$\begin{aligned} L &= [(abc)(dea) - (\underline{aba})(dec)][(bcf)(efd) - (bcd)(\underline{eff})] \\ &\quad - [(abf)(\underline{ded}) - (abd)(def)][(\underline{bcc})(efa) - (bca)(efc)] \\ &= (abc)(def)[(ade)(bcf) - (adb)(ecf)] \\ &= P \cdot (abc)(def). \end{aligned}$$

For the underscored determinants vanish identically. Hence P is a factor of L, and the latter becomes zero with the former,— the fact which was to be proved.

Noticing the other factors of L, we observe that L vanishes also without P when either the three points $A\ B\ C$ or the three points $D\ E\ F$ are collinear; as is evident geometrically, for when the three lines of either triangle coincide, their three intersections with the sides of the other triangle must lie in this triply-counting line.

3. The inscribed hexagon,—Pascal's Theorem. Pascal's theorem may be stated in this form:

If the conic through five vertices of a hexagon contains also the sixth vertex, then the three intersections of pairs of opposite sides of the hexagon will lie in a right line, and conversely.

For proof we shall write down the condition that the three points lie on a line, and show that it is identically the condition that the sixth vertex may lie on the conic determined by the other five.

Designate the vertices by A, B, C, D, E, X, with coordinates respectively (a_1, a_2, a_3) , (b_1, b_2, b_3) . . . . . (x_1, x_2, x_3). Pairs of opposite sides are the lines XA, CD; AB, DE; BC, EX. For their three points of intersection to lie upon a line, the necessary and sufficient condition is the vanishing of a determinant, namely:

$$\begin{vmatrix} (xa,\ cd)_1 & (ab,\ de)_1 & (bc,\ ex)_1 \\ (xa,\ cd)_2 & (ab,\ de)_2 & (bc,\ ex)_2 \\ (xa,\ cd)_3 & (ab,\ de)_3 & (bc,\ ex)_3 \end{vmatrix} \equiv K = 0.$$

The equation $K=0$, is of second degree in the coordinates of X; hence the condition is satisfied for all points X of a certain conic. *This conic is the one which contains the five other points, for K vanishes when X coincides with either A, B, C, D, or E.*

(1) When X coincides with A or E, line-coordinates $(xa)_1$, $(xa)_2$, $(xa)_3$ in the first column of K or $(ex)_1$, $(ex)_2$, $(ex)_3$ in the last column will all vanish, whence $K=0$.

(2) When X coincides with B or D, say with B; expand the determinant K, distributing the constituents of the second column. After replacing x_1, x_2, x_3 by b_1, b_2, b_3 we find:

$$K=\begin{vmatrix}(ba)_1 & (cd)_1 & (de)_1\\ (ba)_2 & (cd)_2 & (de)_2\\ (ba)_3 & (cd)_3 & (de)_3\end{vmatrix}\cdot\begin{vmatrix}(ab)_1 & (bc)_1 & (eb)_1\\ (ab)_2 & (bc)_2 & (eb)_2\\ (ab)_3 & (bc)_3 & (eb)_3\end{vmatrix}$$

$$-\begin{vmatrix}(ba)_1 & (cd)_1 & (ab)_1\\ (ba)_2 & (cd)_2 & (ab)_2\\ (ba)_3 & (cd)_3 & (ab)_3\end{vmatrix}\cdot\begin{vmatrix}(de)_1 & (bc)_1 & (eb)_1\\ (de)_2 & (bc)_2 & (eb)_2\\ (de)_3 & (bc)_3 & (eb)_3\end{vmatrix}.$$

The second of these four determinants vanishes because the three lines concerned meet in one point, B; the third vanishes because two columns differ only in sign. Hence again $K=0$.

(3) When X coincides with C, the first and last columns in K become proportional; for in the first, $(ca, cd)_1 = -(a\,c\,d)c_1$, etc.; and in the last, $(bc, ec)_1 = -(b\,c\,e)c_1$, etc.

Hence the locus of X contains all five other points, and is the conic determined by them, as asserted by the theorem to be proved.

For a class exercise, it is worth while to obtain further Brianchon's theorem by arguing from duality or by exactly parallel reasoning with lines in place of points. The three theorems then gain in interest by being combined in the following:

If a hexagon be inscribed in a conic, its alternate sides intersect in six points which are in corresponding order the vertices of a hexagon circumscribed to a second conic.

[*Postscript:* For a proof of Desargues' theorem closely related to the one given above, see a paper by Hunyady, *Crelle* Vol. 89, p. 79.]

EVANSTON, ILL., DECEMBER, 1899.

ON THE VOLUME OF A POLYHEDRON.

By H. B. Newson.

Many elementary text books on analytical geometry give a formula for finding the area of a plane polygon of n sides in terms of the coordinates of the n vertices. A similar formula exists for finding the volume of a polyhedron of n faces. In the present paper I present a method for deducing these formulas which I have frequently used in my classes, and find well suited for the purposes of instruction. It may be noted that this method applies not merely to ordinary convex polyhedrons, but to any solid bounded by a finite number of plane faces.

1. Area of a polygon of n sides. Let the vertices of a triangle be numbered 1, 2, 3; and let the rectangular cartesian coordinates of these vertices be denoted respectively by (x_1, y_1), (x_2, y_2), (x_3, y_3). Let A denote the area of the triangle. Then by a well-known formula we have:

$$2A = \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} \equiv \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} + \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} + \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix}. \qquad (1)$$

The area of the triangle is here expressed as the sum of three determinants which, so to speak, correspond to the three sides of the triangle. The determinant $\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$ corresponds to the side (1, 2) taken in the sense from 1 to 2, and similarly for the other sides. Thus twice the area of the triangle is found by writing down the sum of the determinants corresponding to the sides of the triangle, taken all in the same sense around the triangle. The law of the formation of the determinants may also be expressed by the convention of a moving point describing the perimeter of the triangle.

We can now apply this result to the problem of finding the area of a polygon of n sides. Let the vertices of the polygon be numbered in order 1, 2, 3, . . ., n, and let the coordinates of the vertex k be denoted by (x_k, y_k), $(k = 1, 2, 3, \ldots, n)$. Let us divide the polygon into a number of triangles, and let a moving point describe the perimeter of each triangle always in the same sense. It is evident that by this process each of the interior

lines will be described twice, but the two descriptions are always in opposite senses; while each of the bounding lines is described once, and always in the same sense. In taking the sum of all these triangles, the two determinants corresponding to the two descriptions of an interior line in opposite senses differ only in sign, and hence cancel each other. Thus we have for twice the area of the polygon, the sum of the determinants corresponding to the sides of the polygon. The formula is therefore:

$$2A = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} + \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} + \begin{vmatrix} x_3 & y_3 \\ x_4 & y_4 \end{vmatrix} + \cdots\cdots + \begin{vmatrix} x_{n-1} & y_{n-1} \\ x_n & y_n \end{vmatrix} + \begin{vmatrix} x_n & y_n \\ x_1 & y_1 \end{vmatrix}. \qquad (2)$$

It may be remarked that each of the determinants in this formula represents twice the area of the triangle formed by joining the origin to two adjacent vertices of the polygon.

2. Volume of a polyhedron of n faces. In like manner if the vertices of a tetrahedron be numbered 1, 2, 3, 4; and if the corresponding coordinates be written (x_1, y_1, z_1), etc., we know, V being the volume of the tetrahedron, that:

$$6\,V = \begin{vmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{vmatrix} \equiv \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} + \begin{vmatrix} x_1 & y_1 & z_1 \\ x_4 & y_4 & z_4 \\ x_2 & y_2 & z_2 \end{vmatrix} + \begin{vmatrix} x_1 & y_1 & z_1 \\ x_3 & y_3 & z_3 \\ x_4 & y_4 & z_4 \end{vmatrix} + \begin{vmatrix} x_2 & y_2 & z_2 \\ x_4 & y_4 & z_4 \\ x_3 & y_3 & z_3 \end{vmatrix}. \qquad (3)$$

Thus we have six times the volume of the tetrahedron expressed by the sum of four determinants which may be said to correspond to the four faces of the tetrahedron. The law of the formation of these determinants may be expressed as follows: let us suppose the perimeter of each face of the tetrahedron to be described by a moving point, and all in the same direction. In determining directions in this case it is supposed that the moving point is always on the external side of the faces of the tetrahedron. The best way for the reader to realize this law is to take in his hand a wooden model of a tetrahedron whose vertices have been numbered 1, 2, 3, 4; and then with each face in turn before him write down the corresponding determinant going around the faces always in the same direction.

A polyhedron of any number of faces can always be decomposed by internal planes into a number of tetrahedrons. Let us find by the above formula the volume of each of these tetrahedrons and take their sum. We readily see that any face of one of these tetrahedrons which is not a part of the bounding

surface of the polyhedron is described twice, but each time in opposite directions, while each face which is a part of the bounding surface is described only once, and all of them in the same direction. The two determinants corresponding to the description of an internal face in opposite directions differ only in sign and hence cancel each other. We have, therefore, the following theorem:

Six times the volume of a polyhedron is equal to the sum of all the determinants corresponding to the triangles which form its bounding surface, each triangle being described in the same direction.

If one or more of the faces of the polyhedron be polygons, each such polygon must be divided into triangles.

Each of these determinants of the third order represents six times the volume of the tetrahedron formed by joining the origin to the vertices of a face triangle.

3. Area of a closed curve. Formula (2) for the area of a polygon may be expressed more concisely as follows:

$$A = \tfrac{1}{2} \sum \begin{vmatrix} x_k & y_k \\ x_{k+1} & y_{k+1} \end{vmatrix} \qquad (k = 1, 2, 3, \ldots, n).$$

We may consider a closed curve as a polygon of an infinite number of sides. The coordinates of two adjacent vertices may be expressed by (x, y) and $(x+dx, y+dy)$ and the determinant $\begin{vmatrix} x_k & y_k \\ x_{k+1} & y_{k+1} \end{vmatrix}$ reduces to $\begin{vmatrix} x & y \\ dx & dy \end{vmatrix}$. Replacing the summation sign by the sign of integration we have,

$$A = \tfrac{1}{2} \int_c (x dy - y dx),$$

a well-known formula for finding the area of a closed curve.

In order to complete this investigation in a symmetrical manner we should deduce from the above theorem for the volume of a polyhedron an integration formula for finding the volume of a closed surface. This I have not been able to do to my satisfaction, and I leave the problem with the readers of the ANNALS.

LAWRENCE, KANSAS, SEPTEMBER, 1899.

A GRAPHICAL METHOD OF DEDUCING THE CRITERIA FOR THE NATURE OF THE ROOTS OF CUBIC AND QUARTIC EQUATIONS.

By R. E. Gaines.

Let the cubic equation be:

$$x^3 + 3Hx + G = 0.^* \tag{1}$$

Forming the simultaneous equations:

$$y = x^3, \tag{2}$$
$$y = -3Hx - G, \tag{3}$$

we have two loci the abscissæ of whose intersections are the roots of (1). Now if a tangent to (2) at the point $(x'\,y')$ be made to pass through $(0, -G)$, its equation $y - y' = 3x(x'^2 - x')$ easily reduces to:

$$y = 3(G/2)^{\frac{1}{3}}x - G. \tag{4}$$

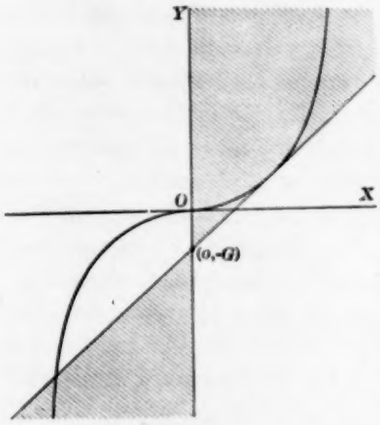


Fig. 1.

Since the right lines (3) and (4) both pass through $(0, -G)$, a comparison of their directions together with the sign of G will give us complete criteria for the nature of the roots of (1). Whether G be positive or negative (see figure 1 as it stands and also turned upside down) one root will be real and the other two will be real and distinct, real and coincident, or imaginary according as (3) lies in the shaded portion of the plane, coincides with the tangent, or lies in the unshaded portion, *i. e.* according as $4H^3 + G^2 <, =, > 0$. Moreover the sign of G will at once determine the signs of the real roots.

The extension of this method to the quartic $x^4 + 6ax^2 + 4bx + c = 0$ is so obvious that the work in detail may be left to the reader. The auxiliary loci

---

* The method we are about to use applies to the general cubic; but for simplicity we take this reduced form.

are a right line and a quartic. The latter, whose equation is $y = x^4 + 6ax^2$, will assume different forms (see figures 2 and 3) according as a is positive or negative. It will be noticed that not only the origin but also the points M

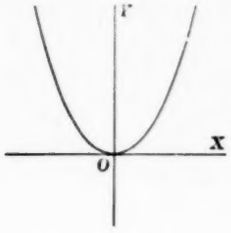


FIG. 2. $a \geqq 0$.

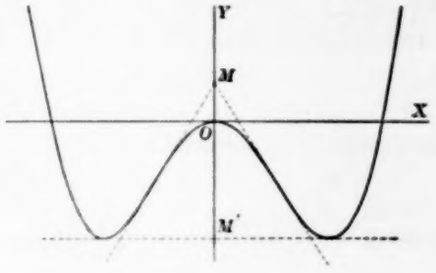


FIG. 3. $a < 0$.

and M', where the Y-axis is met by the tangents at the inflexions and the double tangent respectively, are critical points of this axis.

RICHMOND COLLEGE, VA., DECEMBER, 1899.

GALOIS' THEORY OF ALGEBRAIC EQUATIONS.*

PART I. RATIONAL RESOLVENTS.

By James Pierpont.

Introduction.

If we look over the solutions of the various algebraic equations obtained by the ordinary methods, we observe that they all have this in common: the solution of the given equation $f(x)=0$ is made to depend upon a number of simpler equations:

$$f_1(x)=0,\quad f_2(x)=0,\ \ldots\ldots$$

called resolvents. Such a system of resolvents is obtained in each case by more or less artificial and ingenious methods, and each new equation requires for its solution the invention of a new method.

The Galois theory proposes a general and uniform method of finding these resolvents, free from all artifice. It shows that every equation has an infinite number of such systems and makes clear their relations to one another. In every case it indicates how they may be found by a finite number of operations. If the equation can be solved algebraically, *i. e.* by the extraction of roots from known quantities, this fact is made manifest as well as the manner in which the solution is to be effected. If an algebraic solution is impossible, it shows us what fundamental irrationalities must be introduced, in terms of which the roots can be expressed.

Galois' theory is a combination of two theories: the theory of rational functions of several variables, and the theory of substitution groups. Its chief claim to our attention is the broad and clear insight it affords us into the nature of algebraic irrationalities and their mutual relations.

We propose to develop the subject by giving the reader in Part I a rapid *aperçu* of the theory as a whole; in Part II we shall return to take up certain more difficult points, or questions of detail which are better treated after one has the main features in mind. The first part is complete in itself and will give the reader who does not care to go further the most essential principles of the subject.

---

*The following pages consist of a reproduction, with slight alterations, of parts of a course of lectures delivered in September 1896 at the *Buffalo Colloquium* held under the auspices of the American Mathematical Society.

Preliminary Algebraic Ideas.

1. The coefficients. These are either constants or variables. As variables several cases are possible. For example, they may be independent variables, or they may be rational functions of other variables. These last may themselves be independent or related by algebraic equations.

Examples. 1°. The equation defining the imaginary fifth roots of unity:

$$x^4 + x^3 + x^2 + x + 1 = 0. \tag{a}$$

Here all the coefficients are constants.

2°. The equation defining $x = \tan \phi/4$ in terms of $t = \tan \phi$:

$$x^4 + \frac{4}{t}x^3 + 6x^2 - \frac{4}{t}x + 1 = 0. \tag{b}$$

Here two of the coefficients are rational functions of the independent variable t, the other two are constant.

3°. The equation defining $x = \wp(u/2, g_2, g_3)$ in terms of $p = \wp(u)$:

$$x^4 - 4px^3 + \tfrac{1}{2}g_2x^2 + x(2g_3 + pg_2) + (\tfrac{1}{16}g_2^2 + pg_3) = 0. \tag{c}$$

The coefficients are here rational functions of three independent variables t, g_2, g_3.

4°. An equation whose coefficients are *independent variables* is got by taking n such variables $a_1, a_2, \ldots a_n$, and building the equation:

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0. \tag{d}$$

Definition. The equation (d) is said to be the *general equation* of degree n.

5°. Examples of equations whose coefficients are rational functions of variables which themselves are related by algebraic equations may be found in §§ 34, 35, 36.

2. Domain of Rationality. This notion is one of the most important in the whole theory. Let $\lambda, \mu, \nu, \ldots \omega$ be certain constants or variables finite in number. The quantities which can be formed from these by a finite number of additions, subtractions, multiplications, and divisions form a system which we call a *domain of rationality* and denote by R, or more explicitly by $R(\lambda, \mu, \nu, \cdots \omega)$.

Examples. 1°. The domain $R(1)$. This embraces the rational numbers. Every domain must contain this one. For if R be any domain and λ any element in it, then by definition $\lambda/\lambda = 1$ is in R, and hence all rational numbers,

i. e. $R(1)$, are contained in R. For this reason R (1) is sometimes called the absolute domain.

2°. Let $\epsilon_\kappa = e^{2\pi i\kappa/5}$, $\kappa = 1, 2, 3, 4$ be the roots of (a) in § 1. With any one of these, say ϵ_1, we can generate a domain $R = R(\epsilon_1)$. Consider also the domain $R' = R'(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$. Apparently R' is larger than R; they are however identical. For, every element of R is evidently in R'; on the other hand since $\epsilon_2, \epsilon_3, \epsilon_4$ are only $\epsilon_1^2, \epsilon_1^3, \epsilon_1^4$, these lie in R.

Definition. When all the elements of a domain R lie in a domain R' we say R *is contained or lies in* R'; symbolically $R = R'(R, \ldots)$.

3°. As a final example take $g_2, g_3\, p$, of §1, 3°. These form a domain $R(g_2, g_3, p)$ which contains the coefficients of (c).

Other examples in great number will occur in the following pages.

Definition. When certain quantities $\xi, \eta, \ldots$ do not lie in $R = R(\lambda, \mu, \ldots \omega)$ we may enlarge R by *adjoining* them, generating the new domain $R' = R'(\lambda, \mu, \ldots \omega, \xi, \eta, \ldots) = R'(R, \xi, \eta, \ldots)$.

3. Rational functions for R. In elementary algebra and in the function theory, a rational function of certain quantities $u, v, w, \ldots$ is the quotient of two expressions of the type

$$\Sigma\, C\, u^a v^b w^c \ldots \tag{1}$$

where $a, b, c, \ldots$ are positive integers, and the C's are constants or quantities independent of $u, v, w, \ldots$ Observe that the $u, v, w, \ldots$ may be constants or variables.

Now in Galois' theory the term *rational* has a narrower sense. It is never used except in connection with a domain of rationality.

Definition. An *integral rational function of* $u, v, w, \ldots$ *for the domain* R is an expression of the type (1) where the C's lie in R. The quotient of two integral rational functions is a *rational* function.

In the future we shall use these terms in this sense only.

Definition. All quantities lying in a domain of rationality are said to be *rationally known* with respect to that domain.

Thus if $p, q, r, \ldots$ be certain quantities, constants or variables, which lie in R, any rational function as $\phi(p, q, r \ldots)$ is rationally known with respect to R. But it frequently happens that rational functions of certain quantities $p, q, \ldots$ are rationally known although $p, q, \ldots$ themselves do not lie in the domain in question.

Examples. 1°. Consider equation (d) of § 1. Let its roots be $x_1, x_2, \ldots x_n$. As domain of rationality take $R(a_1, a_2, \ldots a_n)$. Then certainly $x_1, x_2, \ldots x_n$ are not rationally known. But any rational symmetric function $\phi(x_1, x_2 \ldots x_n)$ of the roots is rationally known, since ϕ is a rational function of the coefficients $a_1, \ldots a_n$.

In this connection, we will prove the elementary

THEOREM. *Let R be a given domain, and*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

an equation whose coefficients lie in R. Let its roots be $\xi_1, \xi_2 \ldots \xi_n$. Then an integral rational symmetric function of $n-1$ of the roots, say $\xi_2, \xi_3 \ldots \xi_n$, is an integral rational function of the remaining root ξ_1.

In order to prove this we note that in the quotient

$$g(x) = \frac{f(x)}{x - \xi_1} = x^{n-1} + \beta_1 x^{n-2} + \beta_2 x^{n-3} + \cdots + \beta_{n-1}$$

the coefficients β are integral rational functions of ξ_1 with respect to R. This is seen by multiplying both sides by $x - \xi_1$ and equating the coefficients of like powers of x. Hence $g(x) = 0$ is an equation whose coefficients lie in $R' = R'(R, \xi_1)$. An integral rational symmetric function of its roots $\xi_2, \xi_3 \ldots \xi_n$ lies in R', and is, moreover, integral with respect to ξ_1.

2°. Consider (a), § 1. Take $R(1)$ as domain. For this domain $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$ are certainly not rationally known. But here not only are the rational symmetric functions of the ϵ's rationally known, but a large class of other rational functions. For example

$$\phi(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4) = \epsilon_m \epsilon_{5-m} \qquad m = 1, 2, 3, 4.$$

In fact $\epsilon_m \epsilon_{5-m} = 1$, which of course lies in $R(1)$.

Definition. An equation is said to be a *rational equation* with respect to a domain R, when its coefficients lie in R.

4. Reducibility and Irreducibility. *Definition.* Let $F(x,y,z, \ldots)$ be an integral rational function of the independent variables $x, y, z, \ldots$ with respect to a domain R. We say F is *reducible* for R when there exist two integral functions $G(x, y, z, \ldots)$, $H(x, y, z, \ldots)$, rational with respect to R, such that $F = GH$. G and H are called *rational divisors* or *factors* of F. When no such functions exist F is *irreducible.* Observe that the above definition, depending essentially upon the notion of a rational function, has no sense

unless taken in connection with a definite domain. As we shall see, we commonly use several domains in one and the same course of reasoning. The beginner often forgets that results valid for one domain do not necessarily hold true for another on account of the relativity of the ideas we have just introduced. In this way great confusion may arise. A little care at first, which soon becomes a habit, will prevent this.

Examples. For simplicity take a single variable.

1°. For $R(1)$, $F(x) = x^2 + 1$ is a rational function of x. For $R(1)$ it is irreducible. For if reducible, it must split up into two rational factors $x + a$, $x + b$. On solving $F(x) = 0$ we see that its factors are $x + i$, $x - i$. This shows that $F(x)$ is reducible in $R(i)$.

2°. For $R(1)$, $F(x) = x^2 + x + 1$ is irreducible. For $R'(\rho)$, $\rho = e^{2\pi i/3}$, it is reducible, since $F = (x - \rho)(x - \rho^2)$.

The notion of reducibility plays an absolutely fundamental rôle in Galois' theory. At every turn we are met by the question: is an integral rational function $F(u, v, w, \ldots)$ reducible with respect to R, or not? If it be reducible, we want to find its irreducible factors.

We owe to Kronecker a method whereby we can decide by a finite number of rational operations whether F is reducible or not; if it is reducible the method gives us its irreducible factors, and shows that this decomposition of F into irreducible factors is unique.

Observe that these facts are generalizations of the corresponding ones for integers. In arithmetic we are taught to decide whether a given integer is prime or not; and if not prime, to find its prime factors. This decomposition into prime factors is also unique. In Part II we propose to take up this subject. For the present it will suffice to take as definition of reducibility the *logical* one just given.

Definition. The domain of rationality being R, the rational equation $f(x) = 0$ is said to be *reducible* when $f(x)$ is reducible; otherwise $f(x) = 0$ is an *irreducible equation.*

THEOREM. *Let $f(x) = 0$, $g(x) = 0$ be rational equations for the domain R, and let $f(x) = 0$ be irreducible for this domain. If $g(x) = 0$ admits one root of $f(x) = 0$, it admits all the roots of $f(x) = 0$. The function $g(x)$ admits $f(x)$ as a rational divisor.*

For let:

$$f(x) = (x - \xi_1) \cdots (x - \xi_m), \quad g(x) = (x - \eta_1) \cdots (x - \eta_n).$$

If some of the ξ's are equal to some of the η's, say $\xi_1 = \eta_1 , \ldots \xi_r = \eta_r$, then

$$h(x) = (x - \xi_1) \cdots (x - \xi_r)$$

is a divisor of f and g; it is in fact the greatest common divisor of f and g. But elementary algebra teaches how such a divisor may be found and the method employed shows that the coefficients of $h(x)$ lie in R, *i. e.*, $h(x)$ is a rational divisor of $f(x)$. Hence $f(x) = h(x)\, k\,(x)$, where k is a rational integral function of x. If now k be not of zero degree, *i. e.* a constant, $f(x)$ is reducible. This is contrary to hypothesis. Hence, k being a constant must equal 1. Hence $f(x) = h(x)$ and this is a rational divisor of $g(x)$. Therefore $g(x) = 0$ admits all the roots of $f(x) = 0$.

5. Equality. Before leaving these preliminary algebraic notions we must state clearly what we mean by the terms equal and unequal.

As long as the quantities we are dealing with are constants, equality and inequality are of course the same as in arithmetic — they are *numerical*. What do we mean however by the equation

$$\phi(p, q, \ldots) = \psi\,(p, q, \ldots)$$

ϕ, ψ being rational functions of the variables p, q . . . for a domain R? In general R will contain variable elements which then may enter the coefficients of ϕ, ψ. Let us write the above equation as follows:

$$\phi\,(v_1, v_2, \ldots c_1, c_2, \ldots) = \psi\,(v_1, v_2 \ldots c_1, c_2 \ldots), \tag{1}$$

where v_1, v_2 . . represent now all the variable elements in ϕ, ψ, among which will be p, q. . . . , while c_1, c_2, . . . represent constants.

Definition. By an equation of the type (1) we mean that for each and every set of numerical values v_1, v_2, . . . can take on, consistent with their definition, the resulting numerical value of ϕ is identical with that of ψ.

When no two of the quantities ϕ, ψ, χ, . . . are equal we shall call them *distinct*. In Part II we shall show how to determine by a finite number of operations whether two rational functions ϕ, ψ are distinct or not.

Substitutions.

6. Definitions and first principles. Suppose we have n things, or elements. To distinguish them, we may represent them by marks as a, b, c, . . . or by 1, 2, . . . n.

The operation which replaces a by any one of these n elements, say by a', b

by any one of the remaining $n-1$ elements, say by b', etc. is called a substitution and is represented by

$$s = \begin{pmatrix} a & b & c & \dots \\ a' & b' & c' & \dots \end{pmatrix}.$$

Example. As elements let us take the four roots of a biquadratic equation, x_1, x_2, x_3, x_4. Consider any rational function, say

$$\phi = x_1 x_2 + x_3 x_4.$$

The operation

$$s = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_1 & x_2 & x_4 \end{pmatrix}$$

converts ϕ into $x_3 x_1 + x_2 x_4$ which we may represent by ϕ_s.

The substitution

$$t = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \end{pmatrix}$$

converts ϕ into $\phi_t = x_2 x_1 + x_4 x_3$.

THEOREM. *The number of substitutions on n things is n!*

For, to every permutation of these n things will correspond a substitution.

Example. Take $n = 3$, and represent the elements by 1, 2, 3. The $3! = 6$ permutations are 1 2 3, 1 3 2, 2 1 3, 2 3 1, 3 1 2, 3 2 1, giving the substitutions

$$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$s_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad s_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad s_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

In a substitution we can leave out an element which occurs twice in the vertical line. Thus we can write

$$s_2 = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \qquad s_3 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

In writing down a substitution it is customary to write the top row in a natural order, but this is not necessary. Thus

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

indicate the same operation, viz.: that 1 is to be replaced by 2, 2 by 1, 3 by 3.

Identical substitution. We observe that s_1 leaves every element unchanged. Such a substitution we call in general an *identical substitution.*

Product. If we effect first a substitution s, and then a substitution t, the result of the two is a substitution u. We say u is the product of s and t and write $u = st$; the order of the factors from left to right indicating the order in which the operations are effected.

Similarly $z = s\,t\,y$ is the substitution which arises when we apply first s, then t and finally y. As $s\,t = u$ we can also write $z = u\,y$.

Examples. $s_1, s_2 \cdot \cdot \cdot \cdot s_6$ being the above substitutions we have

$$s_2\,s_5 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = s_6,$$

$$s_2\,s_5\,s_4 = s_2\,s_5 \cdot s_4 = s_6 \cdot s_4 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = s_2.$$

Let $\psi = x_1 + 2x_2 - 5x_3$. As no ambiguity can arise, we can represent a substitution on these roots as

$$\begin{pmatrix}x_1&x_2&x_3\\x_{i_1}&x_{i_2}&x_{i_3}\end{pmatrix} \text{ by } \begin{pmatrix}1&2&3\\i_1&i_2&i_3\end{pmatrix}$$

where $i_1\ i_2\ i_3$ are 1, 2, 3 in a certain order. Then

$$\phi_{s_2} = x_1 + 2x_3 - 5x_2, \quad \phi_{s_2 s_5} = x_3 + 2x_2 - 5x_1 = \phi_{s_6}, \quad \phi_{s_2 s_5 s_4} = x_1 + 2x_3 - 5x_2 = \phi_{s_2}.$$

Notation for identical substitution. If in any product of substitutions $p = st \cdot \cdot w$ one of the factors is the identical substitution, this factor evidently has no effect on the result. It plays, thus, a rôle analogous to unity in a product of numbers. For this reason it is convenient to designate the identical substitution by the symbol 1.

Powers. The product $s \cdot s$ is represented also by s^2, similarly s^3 stands for $s\,s\,s = s^2 \cdot s = s \cdot s^2$ etc.

Observe that multiplication of substitutions is *associative*. In symbols $st.u = s \cdot t\,u$.

Multiplication is not, however, in general *commutative*, that is $s\,t \neq t\,s$ in general. This is shown by simple examples. Thus

$$s_2 s_5 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = s_6 \qquad s_5 s_2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = s_3.$$

Order of a substitution. Consider the indefinite sequence

$$s,\ s^2,\ s^3,\ s^4, \ldots \ldots$$

where s is a substitution on n elements. As the number of such substitutions is $n!$, *i. e.* finite, not all the above substitutions can be distinct. Say $s^a = s^b$;

let $\beta = \alpha + m$. Then $s^{\alpha} = s^{\alpha+m} = s^{\alpha} \cdot s^{m}$; that is, s^{m} leaves s^{α} unchanged. Hence $s^{m} = 1$. If m is the *least* integer for which $s^{m} = 1$, m is called the *order* of s. Then $1, s, s^2, s^3, \ldots s^{m-1}$ are distinct.

Inverse substitution. If $i_1, i_2, \cdots i_n$ represent a permutation of $1, 2, \cdots n$, any substitution on the n elements $1, 2, \cdots n$ is represented by

$$s = \begin{pmatrix} 1, & 2, & 3, & \ldots & n \\ i_1 & i_2 & i_3, & \ldots & i_n \end{pmatrix}.$$

To every substitution s corresponds one and only one substitution t, such that $st = 1$, viz.,

$$t = \begin{pmatrix} i_1, & i_2, & \ldots & i_n \\ 1, & 2, & \ldots & n \end{pmatrix}.$$

Example. $n = 5$, $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$, then $t = \begin{pmatrix} 3 & 1 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$.

Evidently if $st = 1$, we have also $ts = 1$. The substitution t corresponding to s so that $st = ts = 1$ is called the *inverse substitution* and is denoted by s^{-1}. Then $s\,s^{-1} = s^{-1}\,s = 1$.

THEOREM. *From $a\,b = a\,c$ we have $b = c$.*

For, multiplying left handed by a^{-1}, the first equation gives $a^{-1}a \cdot b = a^{-1}a \cdot c$ or $b = c$. Similarly from $b\,a = c\,a$ we infer that $b = c$.

Cycles. Substitutions like $s = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,5\,1 \end{pmatrix}$ or $t = \begin{pmatrix} 3\,2\,5\,1\,4\,7\,6 \\ 2\,5\,1\,4\,7\,6\,3 \end{pmatrix}$ which replace the first element in the top row by the second, the second by the third and so on till finally the last element of the top row is replaced by the first, are called *cycles* or *circular substitutions*. We can represent them more shortly; in fact,

$$\begin{pmatrix} a & b & c & d & \ldots & k & l \\ b & c & d & \ldots & l & a \end{pmatrix} \text{ we write } (a\,b\,c\,d\,\ldots\,l).$$

Then $s = (1\,2\,3\,4\,5)$, $t = (3\,2\,5\,1\,4\,7\,6)$. Observe that it is immaterial where we begin to write a cycle, if we only preserve the relative order of the marks. Thus for example $t = (1\,4\,7\,6\,3\,2\,5)$.

A simple reflection shows that every substitution can be represented as a product of cycles.

Thus $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 4 & 3 & 10 & 6 & 11 & 9 & 5 & 1 & 2 & 8 \end{pmatrix} = (1\ 7\ 9)(2\ 4\ 10)(3)(5\ 6\ 11\ 8)$.

7. Substitution Groups. Let $s_1, s_2, \cdots s_m$ be a system of distinct substitutions such that the product of any two of them is a substitution of the system. Such a system is called a *group*; we denote it by $G = \{s_1, s_2, \cdots s_m\}$. The number m of substitution in G is called its *order*; if its substitution affect n elements G is of *degree* n.

Examples. 1°. The $n!$ substitutions which can be made on n things. This group is called the symmetric group. We denote it by S_n. Such a group is $\{s_1 = 1, s_2, s_3, s_4, s_5, s_6\}$ of the last paragraph. It is of order 6 and degree 3.

Definition. Let $\phi(x_1 \cdots x_n)$ be a rational function of the roots of an equation. Apply to ϕ a substitution s. If $\phi_s = \phi$ we say s leaves ϕ *unaltered* or *unchanged*; otherwise s *alters* or *changes* ϕ.

The substitutions of the symmetric group leave every rational symmetric function of $x_1, x_2, \cdots x_n$ unaltered; whence the name of this group.

2°. Let s be any substitution of order m. Then

$$1, s, s^2, \cdots s^{m-1}$$

form a group of order m, which is called a cyclic group.

Thus if $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1\,2\,3)(4\,5)$, then

$$1,\ s,\ s^2 = (1\,3\,2),\ s^3 = (45),\ s^4 = (123),\ s^5 = (132)(45)$$

form a cyclic group of order 5 and degree 5.

3°. The substitutions K, common to two groups G, H, form a group. For if a, b are common to G, H, so is their product $a\,b$.

Every group G contains the identical substitution. For if s be any substitution of G, $s^2, s^3 \ldots$ are in G. But, for some power, $s^m = 1$. If s be any substitution of G so is s^{-1}. For, let s be of order m; then $s^{-1} = s^{m-1}$.

Subgroups. Let $G = \{a = 1, b, c, \cdots l, \alpha, \beta, \cdots\}$ be a group of order g. If certain of its substitutions $a = 1, b, c, \cdots l$ form a group $H = \{a = 1, b, c, \cdots l\}$, H is said to be a *subgroup* of G. Let its order be h. The ratio $g : h = r$ is called the *index* of H under G.

THEOREM. *The index r is an integer.* For, let us form the array,

$$A; \qquad \begin{array}{llll} a = 1 & b & c & \cdots l \\ s_1 & b\,s_1 & c\,s_1 & \cdots l\,s_1 \\ s_2 & b\,s_2 & c\,s_2 & \cdots l\,s_2 \\ \cdots & \cdots & \cdots & \cdots \end{array}$$

as follows. In the first row put the elements of H. Let s_1 be a substitution

of G not in H. With this we form the second row of A as indicated. No two elements of this row are equal. For, if $b s_1 = c s_1$ we have $b = c$ (§6). No element of the second row is in the first row. For, if j be an element of the first row and $k s_1$ an element of the second, so that $j = k s_1$, then $k^{-1} j = s_1$. But $k^{-1} j$ is a substitution of H while s_1 by hypothesis is not. Hence the elements of the first two rows of A are distinct substitutions of G. If these do not exhaust all the elements of G, let s_2 be a new substitution of G. With this we form the third line of A; and these substitutions are different from each other and from the former ones. Continue till all the substitutions of G are exhausted. The array A is then complete; it contains each substitution of G once and once only. The fact that we can form such an array shows that h is a divisor of g.

The Galoisian Resolvent and Group.

8. Construction of n! valued functions. Let

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0 \qquad (A)$$

be an equation to be solved. The first thing to do is to choose a domain of rationality R. The nature of this domain depends partly upon the equation, and partly upon our own pleasure. In any case it must contain the coefficients.

Without loss of generality we can suppose that the roots $x_1, x_2, \ldots x_n$ of (A) are distinct. For, if (A) has equal roots, we can replace it by another equation $g(x) = 0$, whose roots are distinct, got by dividing out from $f(x)$ the greatest common divisor of $f(x)$ and $f'(x)$. The equation $g(x) = 0$ is rational for R.

We wish now to form a $n!$ valued rational function of the roots. To this end we introduce n new variables $u_1, u_2, \ldots u_n$ which we adjoin to R forming the domain R'. Consider the rational function of the roots:

$$V_1 = u_1 x_1 + \cdots + u_n x_n. \qquad (1)$$

Apply the $n!$ substitutions of the symmetric group $S_n = \{s_1 = 1, s_2, \ldots s_{n!}\}$ to it, and let s_κ change V_1 into $V_\kappa = u_{\kappa_1} x_1 + \cdots u_{\kappa_n} x_n$. Build now the equation

$$F(t; u_1, \ldots u_n) = (t - V_1)(t - V_2) \cdots (t - V_{n!}) = 0. \qquad (2)$$

The coefficients, being integral rational symmetric functions of $x_1, x_2, \ldots x_n$, are integral functions of $a_1, \cdots a_n$. They will also contain $u_1, u_2, \ldots u_n$ in an integral way. The equation $F(t) = 0$ is thus a rational equation with respect to R'. The discriminant will be a rational integral function $D(u_1, \ldots u_n)$ of

$u_1, \ldots u_n$ whose coefficients lie in R. In Part II we shall show that it is possible in an infinite variety of ways to give the u's such values $a_1, \ldots a_n$ lying in R, that $D(a_1, \ldots a_n) \neq 0$. The corresponding equation $F(t; a_1, \ldots a_n) = 0$ is now a rational equation for R, and all its roots are distinct. Thus $V_1 = u_1 x_1 + \cdots u_n x_n$ is a $n!$ valued function for an infinite number of sets of values of $u_1, \ldots u_n$ lying in R. Besides this particular function there are an infinity of other $n!$ valued rational functions of the roots of (A) as may be readily shown. For our purpose, V_1 will suffice.

9. Indeterminates. On replacing the u's by the a's these variables disappear. Their introduction was to show the existence of rational functions of the roots of (A) which are $n!$ valued. Such auxiliary variables which we introduce to aid our reasoning, and which at any moment can be made to disappear by giving them appropriate special values, are called *indeterminates*. In a primitive way they are used by all mathematicians. Kronecker has shown that they are an implement of immense power in algebraical speculations. Since in the end we always replace the indeterminates by values lying in our domain, we shall suppose, without further mention, that our domain contains in advance as many of these auxiliary variables as we see fit to use.

10. Galoisian Resolvent. Return to the equation (2), § 8. We will suppose that the u's have been left indeterminate. If (2) is reducible let

$$F(t) = G_1(t; u_1, \ldots u_n)\ G_2(t; u_1, \ldots u_n) \ldots$$

be its decomposition into irreducible factors. Any one of the equations $G_\kappa(t) = 0$ is called a Galoisian Resolvent of (A) for R. A fundamental property of these resolvents is expressed in the

THEOREM: *The roots of (A) are rational in any one of their roots, V_κ.*

For, let $G_\kappa(t) = 0$ be that one of the resolvents which admits $V_\kappa = u_{\kappa_1} x_1 + \cdots + u_{\kappa_n} x_n$ as root. Let its degree be m_κ. The equation $G_\kappa(V_\kappa) = 0$ is an identity in the u's when we take account of the relation (A) between the x's. Differentiate now with respect to u_{κ_i}:

$$\frac{\partial G_\kappa(V_\kappa)}{\partial V_\kappa} \cdot \frac{\partial V_\kappa}{\partial u_{\kappa_i}} + \frac{\partial G_\kappa(V_\kappa)}{\partial u_{\kappa_i}} = 0.$$

But since $\dfrac{\partial V_\kappa}{\partial u_{\kappa_i}} = x_i$, this gives:

$$x_i = -\left\{ \frac{\partial G_\kappa(t; u_1, \ldots u_n)}{\partial u_{\kappa_i}} : \frac{\partial G_\kappa(t; u_1, \ldots u_n)}{\partial t} \right\}_{t = V_\kappa}. \qquad (1)$$

The denominator cannot vanish since $G_\kappa(t)$ has no equal roots. The equation (1) shows that $x_1, \ldots x_n$ are rational in V_κ. On the other hand the V's by definition are rational in the x's. Hence the solutions of $f=0$ and $G_\kappa=0$ are equivalent problems. This justifies the name resolvent. As it is obviously immaterial which of the equations $G_\kappa=0$ we take as resolvent, we shall for convenience of notation take $G_1=0$. We shall call this *the* Galoisian Resolvent and denote it often simply by $G(t)=0$, writing also $m_1=m$.

11. Canonical form of a rational function of one root of an algebraic equation.

THEOREM. *Let R be a given domain and*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{1}$$

be a rational equation whose roots are $\xi, \xi_1, \ldots \xi_{n-1}$. Any rational function $\psi(\xi)$ of one of them, ξ, can be brought to the form

$$\psi(\xi) = \beta_0 + \beta_1 \xi + \cdots + \beta_{n-1} \xi^{n-1}$$

where $\beta_0, \beta_1, \ldots$ lie in R.

For, by virtue of (1), all powers of ξ higher than $n-1$ can be expresssd as integral functions of ξ of degree $< n$; hence the most general form of $\psi(\xi)$ is

$$\psi(\xi) = \frac{a_0 + a_1 \xi + \cdots a_{n-1} \xi^{n-1}}{b_0 + b_1 \xi + \cdots b_{n-1} \xi^{n-1}} = \frac{g(\xi)}{h(\xi)} \tag{2}$$

where the a's and b's lie in R. Multiply numerator and denominator by $h(\xi_1)\, h(\xi_2) \cdots h(\xi_{n-1})$, we have

$$\psi(\xi) = \frac{g(\xi) h(\xi_1) \cdots h(\xi_{n-1})}{h(\xi) h(\xi_1) \cdots h(\xi_{n-1})}.$$

Here the denominator is a symmetric function of all the roots of (1); it is therefore a quantity in R. The factor $h(\xi_1)\, h(\xi_2) \cdots h(\xi_{n-1})$ is an integral symmetric function of $n-1$ of the roots of (1). By the theorem of § 3 it is an integral rational function of ξ.

Corollary. Every rational function $\phi(x_1, \ldots x_n)$ of the roots of (A) can be brought to the form

$$\phi(x_1, \ldots x_n) = r_0 + r_1 V_1 + r_2 V_1^2 + \cdots + r_{m-1} V_1^{m-1} \tag{3}$$

where the r's lie in R.

For, by § 10, all the x's are rational functions of V_1, which is a root of $G(t)=0$ of degree m.

12. Galoisian Group. Let the roots of $G(t)=0$ (1)

be $$V_1, V_2, \ldots V_m; \quad (2)$$

they are derived from V_1 by the substitutions

G; $$s_1 = 1, s_2, \ldots s_m. \quad (3)$$

These substitutions enjoy the following three properties embodied in the

THEOREM: 1°. *Every rational function $\phi(x_1, \ldots x_n)$ of the roots of (A) which remains unaltered for G lies in R, i. e. is rationally known.*

2°. *If $\phi(x_1, \ldots x_n)$ is rationally known it remains unaltered for G.*

3°. *The substitutions G form a group, — the* GALOISIAN GROUP *of (A) for the domain R.*

Proof, 1°. If $\phi(x_1, \ldots x_n)$ remains unchanged for G it lies in R. For, by §11, (3) we can write

$$\phi(x_1, \ldots x_n) = r_0 + r_1 V_1 + \cdots r_{m-1} V_1^{m-1} = \psi(V_1), \quad (4)$$

the r's lying in R. Apply to (4) the m substitutions of G. Since ϕ remains unaltered we have

$$\phi = \psi(V_1) = \psi(V_2) = \cdots \psi(V_m),$$

which gives $$\phi = \frac{1}{m}\{\psi(V_1) + \cdots \psi(V_m)\}. \quad (5)$$

The parenthesis is a rational symmetric function of the roots of (1), and is hence rational in its coefficients *i. e.* ϕ is rationally known.

Remark. This reasoning shows how ϕ may be actually computed in terms of known quantities.

2°. If $\phi(x_1, \ldots x_n)$ lies in R, it is unaltered by G. For, on this hypothesis,

$$\psi(t) - \phi = r_{m-1} t^{m-1} + r_{m-2} t^{m-2} + \cdots r_1 t + (r_0 - \phi) = 0 \quad (6)$$

is a rational equation. By virtue of (4) it admits the root $t = V_1$. Hence (6) admits all the roots of (1). Hence

$$\phi = \psi(V_1) = \psi(V_2) = \cdots \psi(V_m).$$

These equations state that $\phi(x_1, \ldots x_n) = \psi(V_1)$ remains unaltered for G.

3°. The substitutions G form a group. For, consider the integral function of t

$$G(t) = (t - V_{s_1})(t - V_{s_2}) \cdots (t - V_{s_m})$$

which forms the left hand side of (1). Its coefficients lying in R, are unal-

tered by G, by virtue of 2°. On applying a substitution s_κ of G we have then

$$G(t) = (t - V_{s_\kappa})(t - V_{s_2 s_\kappa}) \cdot \cdots \cdot (t - V_{s_m s_\kappa}).$$

This shows that $G(t)$ vanishes for

$$V_{s_\kappa}, V_{s_2 s_\kappa}, \ldots . V_{s_m s_\kappa}.$$

As $G(t)$ does not vanish identically, these quantities are, aside from their order, identical with (2). Moreover V_{s_a} never equals V_{s_b} unless $s_a = s_b$; hence the substitutions s_κ, $s_2 s_\kappa$, ... $s_m s_\kappa$ are, aside from their order, identical with (3). Hence the product of any two substitutions of (3) is a substitution of (3), *i. e.* G forms a group.

It must be kept in mind that the term Galoisian group of an equation has no sense unless taken in connection with a definite domain. We shall sometimes call it *the* group of (A) for R.

Definition. If ϕ, ψ are rational functions for a domain R of the roots of (A), $\phi = \psi$ is called a rational equation or relation between these roots with respect to R.

Corollary. In every rational equation $\phi = \psi$ between the roots of (A) the substitutions of G may be applied and the result is a true equation. For $\phi - \psi$, being equal to zero is a rational function of the roots lying in R and therefore by 2° is unaltered by G.

Remark. While in any rational equation between the roots we can effect a substitution of the Galoisian group it is not true that we can apply a substitution at will, outside of G.

Example. $x^3 - 1 = 0$, $x_\kappa = e^{2\pi i \kappa/3}$, $\kappa = 0, 1, 2$. Take as domain $R(1)$, and as a rational relation $x_1 x_2 = 1$. On applying (0 1 2) this relation goes over into $x_0 x_2 = 1$. This is false as $x_0 x_2 = x_2 \neq 1$.

13. Characteristic properties of the Galoisian Group. The properties 1°, 2° of §12 completely determine the Galoisian group G, *i. e.* any group Γ having these properties is identical with G.

1°. Suppose we know of a group Γ that all rational functions of $x_1, \cdots x_n$ remaining unaltered for Γ lie in R. Then Γ contains G.

For let V_1 take on the values $V_1 = V', V'', V''', \ldots$ for Γ. The equation $H = (t - V')(t - V'') \cdot \cdots = 0$ is rational, since its coefficients are symmetric in $V', V'', \ldots$ and therefore unaltered by Γ. It admits the root $t = V_1$ of $G(t) = 0$; hence $H = 0$ admits all the roots of $G = 0$, *i. e.*

$V_1, V_2, \ldots V_m$ are among the roots of $H=0$; and hence the substitutions of the Galoisian group are in Γ.

2°. Suppose we know of a group Γ that all rational functions of $x_1, \ldots x_n$ lying in R are unaltered for Γ. Then G contains Γ.

For the rational function $G(V')$ lies in R, since its value is zero, and by hypothesis it is unchanged for Γ. Applying the substitutions of Γ to $G(V')=0$ gives:

$$0=G(V')=G(V'')=G(V''')=\ldots.$$

Thus the roots of $H=0$ are among those of $G(t)=0$, and hence Γ is contained in G. 1° and 2° give the

THEOREM: *The Galoisian group for a given domain is unique.*

14. Further properties of the Galoisian Resolvent and Group. From the uniqueness of the group of an equation for a given domain we deduce at once the

THEOREMS: 1°. *The Galoisian group is independent of the particular $n!$ valued function chosen.*

2°. *We get the same Galoisian group whichever resolvent $G_\alpha(t)=0$ we take.*

3°. *The functions $G_\alpha(t)$ are of the same degree.*

15. Determination of the group of the general equation of degree n. Let the coefficients of (A) §8 be independent variables. Then (A) is a general equation. We seek its group.

THEOREM: *For a domain R containing the coefficients and any arbitrary constants, the group of the general equation of degree n is the symmetric group S_n of degree n.*

To prove this we have only to show that $G(t)=0$ is of degree $n!$ In $G(V_1)=0$ replace V_1 and $a_1, \ldots a_n$ by their expressions in the x's. Since the result is an identity in the independent variables, $x_1, \ldots x_n$, we can permute the x's and still have a true equation. Thereby the a's, being symmetric in the x's, remain unaltered, while V_1 goes over into $V_2, V_3, \ldots V_{n!}$. Since $G(t)=0$ admits these V's as roots, its degree is $n!$

16. Criterion for irreducible equations. Transitivity.

Definition. A substitution group on a number of elements, which permits us to replace any one of these elements by any other is called transitive, otherwise intransitive.

THEOREM. *An equation* $f(x) = (x-x_1) \cdot \cdot \cdot \cdot (x-x_n) = 0$ *is irreducible for* R *if its group* G *for this domain is transitive, otherwise* $f(x) = 0$ *is reducible.*

1°. If $f = 0$ is irreducible, G is transitive. For, if intransitive, suppose its substitutions permit us to replace x_1 by $x_1, x_2, \ldots x_m$ but not by $x_{m+1}, \cdot \cdot \cdot \cdot x_n$. Evidently G contains no substitution which replaces an element of the first set by one of the second. Consider now the equation $g(x) = (x-x_1) \cdot \cdot \cdot \cdot \cdot (x-x_m) = 0$. Its coefficients are unchanged by G, hence $g = 0$ is a rational equation. Having one root in common with the irreducible equation $f = 0$, $g(x)$ is divisible by $f(x)$, hence $g = 0$ is identical with $f = 0$.

2°. If G is transitive, $f = 0$ is irreducible. For say $g(x) = (x-x_1) \cdot \cdot \cdot \cdot (x-x_m)$ were a rational factor of $f(x)$. In the rational relation $g(x_1) = 0$ apply the substitutions of G. It goes over into $g(x_\kappa) = 0 \quad \kappa = 1, 2, \ldots n$. Hence $g = 0$ admits all the roots of $f = 0$ and is thus identical with $f = 0$.

17. Group belonging to a rational function of the roots. Let $f(x) = 0$ be an equation whose coefficients lie in a given domain R. Let G be its group for R. Consider now the rational functions of its roots. Some of these, viz., the symmetric functions, will lie in R in every case. Let $\phi(x_1, \ldots x_n)$ be a rational function which does not lie in R. Then it is altered by some of the substitutions of G and unaltered for others.

THEOREM. *The substitutions* $a, b, c, \ldots$ *of* G *which do not alter* ϕ *form a subgroup* H *of* G.

For, by hypothesis, $\phi_a = \phi_b = \phi$. In the rational equation $\phi_a = \phi$ apply b. The result is, by the corollary of §12, a true equation. Hence $\phi_{ab} = \phi_b = \phi$; that is, ab leaves ϕ unaltered and, being in G, is also in H. Hence the substitutions of H form a group. We say H *belongs to* ϕ *or* H *is the group of* ϕ.

Remark. While it is true that the substitutions of the Galoisian group which leave ϕ unaltered form a group, this is not true for substitutions in general.

Example. The substitutions of the symmetric group S_5 which leave the rational function $\phi = x_1 x_3$, where $x_\kappa = e^{2\pi i \kappa/6}$ unaltered do not form a group.

18. Rational functions belonging to a group. *Definition.* A rational function $\phi(x_1, \ldots x_n)$ which is unaltered for a subgroup H of G, but is altered for all other substitutions of G, is said to *belong to* H.

Such functions can be formed without limit. For let V_1 be *any* $n!$ valued

rational function, and t an indeterminate. Let $V_1, \ldots V_r$ be the values V_1 takes on for H. Consider the product:

$$g(t) = (t - V_1) \cdots (t - V_r) = t^r + A_1 t^{r-1} + \cdots + A_r.$$

The coefficients A_κ being symmetric functions of $V_1, \ldots V_r$ are unchanged for H. Hence $g(t)$ is, for all values of t in R, a rational function of the roots $x_1, \ldots x_n$ unaltered by H. But, on properly choosing t, it is altered by every other substitution of G. Let s_λ be such a substitution, $\lambda = r+1, \ldots m$. On applying s_λ, $g(t)$ goes over into $g_\lambda(t) = t^r + A'_1 t^{r-1} + \cdots + A'_r$. As the coefficients of $g - g_\lambda$ are not all zero, we can choose t in these $m-r$ functions so that $g - g_\lambda \neq 0$. For, being polynomials of degree $r-1$ in t, each one of these differences $g - g_\lambda$ can vanish but for $r-1$ values of t; and these we can avoid.

19. Actual determination of the Galoisian Group. As before let $G(t) = 0$ be the Galoisian resolvent for R. The polynomial $G(t)$ may be viewed from two standpoints. By virtue of the expression,

$$G(t) = (t - V_1)(t - V_2) \cdots (t - V_m),$$

where

$$V_\kappa = u_{\kappa_1} x_1 + u_{\kappa_2} x_2 + \cdots + u_{\kappa_n} x_n,$$

we may consider it as an integral rational function $G(t; x_1, \ldots x_n)$ of the indeterminate t and the x's. On the other hand we may consider it as an integral rational function $G(t; u_1, \ldots u_n)$ of t and $u_1, \ldots u_n$.

Considered as a function of the x's, $G(t; x_1, \ldots x_n)$ belongs to the Galoisian Group §§12, 18. Considered as a function of the u's, the group of $G(t; u_1, \ldots u_n)$ is readily found. In fact, consider any substitution s_α of the symmetric group S_n. By definition s_α converts $V_1 = u_1 x_1 + \cdots + u_n x_n$ into $V_\alpha = u_{\alpha_1} x_1 + \cdots + u_{\alpha_n} x_n$.

If we write V_1 in the form $V_1 = u_{\alpha_1} x_{\alpha_1} + \cdots + u_{\alpha_n} x_{\alpha_n}$ we see that s_α must be

$$s_\alpha = \begin{pmatrix} x_{\alpha_1} & \cdots & x_{\alpha_n} \\ x_1 & \cdots & x_n \end{pmatrix}.$$

The inverse substitution s_α^{-1} is $s_\alpha^{-1} = \begin{pmatrix} x_1 \cdots x_n \\ x_{\alpha_1} \cdots x_{\alpha_n} \end{pmatrix}$.

Consider now the substitutions $\sigma_\alpha = \begin{pmatrix} u_1 \cdots u_n \\ u_{\alpha_1} \cdots u_{\alpha_n} \end{pmatrix}$

which we get from s_a^{-1} by replacing there the x's by the u's. The substitution σ_a also converts V_1 into V_a. In particular we observe that the substitutions σ which convert V_1 into $V_1, V_2, \ldots V_m$, the roots of the Galoisian resolvent, are those corresponding to $s_1^{-1} = 1, s^2, \ldots s_m^{-1}$. But these are merely the substitutions of the Galoisian group, $1, s_2, \ldots s_m$ in another order. Hence the substitutions $\Gamma = (\sigma_1, \sigma_2, \ldots \sigma_m)$, and only these, convert V_1 into $V_1, V_2, \ldots V_m$. Therefore a substitution σ_a not in Γ changes the value of $G(t; u_1, \ldots u_n)$, since the corresponding substitution s_a^{-1} changes the value of $G(t; x_1, \ldots x_n)$ which is only $G(t; u_1, \cdots u_n)$ viewed from the other standpoint. Hence to find the group G we seek the group Γ and replace in it the u's by the x's. To find the group Γ we need only to apply the substitutions σ of the symmetric group in the u's to the function $G(t; u_1, \cdots u_n)$ and remember that here $G(t; u_1, \ldots u_n)$, $G(t; u_{a_1}, \ldots u_{a_n})$ are equal or unequal according as they are *formally* equal or not.

There is a trivial ambiguity which arises from the fact that we do not know which one of the factors of $F(x) = G_1(t)\, G_2(t) \cdots$ is $G_1(t)$. The only effect this can produce is that of assigning to the roots their indices in a different order, and this is entirely immaterial.

Application of the Galoisian Group to solve equations. General theory.

20. Reduction of the Group on adjoining $\phi(x_1, \ldots x_n)$. Let ϕ be a rational function of the roots of the given equation (A) which does not lie in R. Let its group be H.

Theorem. *The adjunction of ϕ reduces the Galoisian group of $f(x) = 0$ to H.*

For, let the enlarged domain be $R' = R'(R, \phi)$, and for this domain let T be the Galoisian group sought. Evidently T is contained in G, since T is determined by that irreducible factor of $F(t)$ which admits V_1 as a root, and this is certainly a factor of $G_1(t)$. T can contain no substitution of G not in H, since ϕ, which lies in our present domain R', is altered for such substitutions (§12, 2°). On the other hand T contains H, since all rational functions for R' are of the form $\psi(\phi, R)$, and these are manifestly unaltered for H (§ 13, 2°). Hence $T = H$.

21. Relation between rational functions belonging to same group. Let $\phi(x_1, \ldots x_n)$, $\psi(x_1, \ldots x_n)$ be two rational functions for R

belonging to the same subgroup H of the Galoisian group of $f(x)=0$ for R. Then ϕ and ψ are rational functions of each other. For adjoin one of them, as ϕ. The Galoisian group is now H, the current domain $R'(R,\phi)$. But §12, 1° shows that ψ is a rational function of ϕ for R, since ψ is unchanged for H.

22. Resolvent for ϕ. Let $\phi=\phi_1$ belong to H a subgroup of G of index r. Let the substitutions of H be $1, a, b, c, \ldots$. Then by §7 we can arrange the substitutions of G in the array

$$(A)\qquad \begin{array}{cccccc} 1 & a & b & c & \ldots \\ s_2 & a\,s_2 & b\,s_2 & c\,s_2 & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ s_r & a\,s_r & b\,s_r & c\,s_r & \ldots \end{array}$$

For brevity let $\phi_{s_\kappa}=\phi_\kappa$. These ϕ's are distinct. For, if $\phi_{s_\iota}=\phi_{s_\kappa}$ then $\phi_{s_\iota s_\kappa^{-1}}=\phi$, which requires that $s_\iota s_\kappa^{-1}$ is a substitution h of H. But from $s_\iota s_\kappa^{-1}=h$ we have $s_\iota = h\,s_\kappa$ which is impossible. The substitutions of the row containing s_κ change ϕ into ϕ_κ, and the substitutions of the other rows change ϕ into a ϕ different from ϕ_κ. Hence ϕ takes on exactly the r values $\phi_1,\phi_2,\ldots\phi_r$. These are called *conjugate functions*. Consider the equation:

$$\Phi(y)=(y-\phi_1)\ldots(y-\phi_r)=0.$$

Its coefficients being unchanged for G lie in R. It is thus a rational equation for R. It is irreducible in R. For let $\Psi(y)$ be a rational factor of $\Phi(y)$. In the rational relation $\Psi(\phi_1)=0$ we can apply all the substitutions of G and these change ϕ_1 into $\phi_2,\ldots\phi_r$. Hence $\Psi(y)$ is divisible by Φ, and therefore Φ is irreducible. The equation $\Phi(y)=0$ is a resolvent of the given equation, for, as we shall see, its resolution is a step toward the solution of the given equation.

23. Resolvents for H. The results of § 22 can be looked at from a different standpoint. Let H be any subgroup of G of index r. To it belongs an infinity of rational functions $\phi(x_1,\ldots x_n)$. Any one of them is root of a rational irreducible equation $\Phi(y)=0$. Hence to any subgroup of G belongs an infinite system of rational resolvents.

24. Solution of an equation by rational resolvents. Suppose now we solve one of these resolvents, say $\Phi(y)=0$. Let ϕ be that one of

its roots which belongs to H. This root is now a known quantity. For the domain $R'(R, \phi)$ the group of $f(x) = 0$ is H. As it is a subgroup of G its order is less than that of the original group. But for the domain R' and group H we can reason just as we did for R and G. For let I be a subgroup of H of index s under H. To I belongs an infinite system of rational irreducible resolvents for the domain R', of degree s. Let $\Psi = 0$ be one of these, and let ψ be that one of its roots belonging to I. Suppose we solve $\Psi = 0$; then ψ is a known quantity. The adjunction of ψ produces the domain $R''(R, \phi, \psi)$ for which the group of $f(x) = 0$ is I. Proceed in this way to build resolvents and adjoin their roots. After each adjunction, the group of $f(x) = 0$ is reduced; it finally reduces to the identical substitution.

In this last domain, $R^{(\Delta)}$, lie the roots $x_1, \ldots x_n$. For being unchanged by the substitutions of the present Galoisian Group viz., the identical substitution 1, they must lie in $R^{(\Delta)}$, by § 12, 1°. Hence these roots $x_1, \ldots x_n$ can be got by rational operations on $\phi, \psi, \ldots\ldots$ Theoretically, they can be got as follows. For a particular domain, the degree of the Galoisian resolvent is the same as the order of the Galoisian Group for that domain. Hence when the group has been reduced to the identical substitution, the degree of the corresponding resolvent is one. That is, it has the form $G(t) = t + a = 0$, where a is a known quantity in $R^{(\Delta)}$. But as V_1 is a root of $G(t) = 0$, we have $V_1 = -a$. In § 10 we saw how to get $x_1, \ldots x_n$ rationally from V_1.

25. Adjunction of several of the roots of a rational resolvent. Conjugate groups. In the preceding article we adjoined each time only one root of each resolvent. It is often convenient to adjoin several roots of the same resolvent. The resulting group is easily determined. Turn to the array A in §22, and let us find the substitutions γ of G which leave ϕ_κ unaltered.

Let $\phi_\kappa = \phi_{s_\kappa}$ be unaltered for γ; then $\phi_{s_\kappa} = \phi_{s_\kappa \gamma}$, $\therefore \phi_1 = \phi_{s_\kappa \gamma s_\kappa^{-1}} \cdot \therefore s_\kappa \gamma s_\kappa^{-1} = h$ a substitution of H. $\therefore \gamma = s_\kappa^{-1} h\, s_\kappa$.

Definition. The operation $s^{-1}(\cdot\ \cdot\ \cdot\ \cdot)s$ on a substitution $(\cdot\ \cdot\ \cdot\ \cdot)$ is called transformation by s.

Thus the substitutions of G which belong to ϕ_κ are got from those of H by transforming these by s_κ.

These substitutions

$$H_\kappa; \qquad 1, \quad s_\kappa^{-1} a\, s_\kappa, \quad s_\kappa^{-1} b\, s_\kappa, \quad \ldots$$

form a group; for the product of two of them is

$$s_\kappa^{-1} a\, s_\kappa \cdot s_\kappa^{-1} b\, s_\kappa = s_\kappa^{-1} a \cdot s_\kappa s_\kappa^{-1} \cdot b s_\kappa = s_\kappa^{-1} \cdot ab \cdot s_\kappa$$

which is a substitution of H_κ since ab is a substitution of H. For conformity of notation, set $H = H_1$. The groups

$$H = H_1, \quad H_2, \ldots . H_r,$$

which belong respectively to the conjugate functions

$$\phi = \phi_1, \quad \phi_2, \ldots \phi_r,$$

are called conjugate groups. We sometimes write $H_\iota = s_\iota^{-1} H s_\iota$.

Suppose now, instead of adjoining $\phi = \phi_1$, we adjoin any root, say ϕ_ι of $\Phi(y) = 0$. Then the reasoning of §20 shows that the group after this adjunction is H_ι. Let us adjoin any two roots ϕ_ι, ϕ_κ. The group can now contain no substitution of G which changes either ϕ_ι or ϕ_κ, it must lie in the group of substitutions C, which are common to H_ι and H_κ. Obviously by the reasoning at the close of §20 it contains C .·. the group is C. The same remarks apply when we adjoin any number of the roots of $\Phi = 0$. In each case the resulting Galoisian group is the group of substitutions common to the groups belonging to these functions.

26. Adjunction of all the roots of $\Phi = 0$. Invariant subgroups. This case is of particular interest. The group C corresponding to this case we denote by I. Let its order be e.

Definition. A subgroup B of a group A is an invariant subgroup if it remains unchanged when transformed by all the substitutions of A.

Example. The group 1, (1 2 3), (1 3 2) is an invariant subgroup of the symmetric group in three elements S_3, as is seen by actual trial. Other examples are given in §33.

THEOREM. *The group I is an invariant subgroup of G.*

For let g be a substitution of G, and i one of I. Then $g^{-1} i g$ is in I. For g^{-1} converts any one of the ϕ's, say ϕ_α, into say ϕ_β. This last is unchanged by i; hence it is converted back to ϕ_α on applying g, since g is the inverse of g^{-1}. Hence $g^{-1} i g$ leaves all the ϕ's unchanged and is thus in I.

27. Another solution. Series of composition. *Definition.* If G_1 be an invariant subgroup of G, such that G contains no invariant subgroup containing G_1, it is a *maximum invariant subgroup* of G.

Definition. The series of groups

$$G, G_1, G_2, \ldots G_\lambda = 1$$

such that each is a maximum invariant subgroup of the preceding group, is called a *series of composition of G.*

It is often possible to decompose a group G into a series of composition in several ways.

Example. Take $C_6 = \{1, s = (1\,2\,3\,4\,5\,6), s^2, s^3, s^4, s^5\}$. The subgroups $\Gamma_3 = \{1, s^2, s^4\}$ and $\Gamma_2 = \{1, s^3\}$ are maximum invariant subgroups of C_6. Hence

$$C_6, \Gamma_3, 1 \quad \text{and} \quad C_6, \Gamma_2, 1,$$

are two distinct series of composition of C_6.

These notions established, the following solution of our equation suggests itself. Let G be the Galoisian Group of the given equation. Take a maximum invariant subgroup G_1 of G and build a corresponding resolvent $\Phi_1 = 0$. Since the conjugate groups of G_1 are identical with G_1, the conjugate functions, that is the roots of $\Phi_1 = 0$, are rational in one another. The effect of adjoining one of them is the same as that of adjoining all. After their adjunction the Galoisian group is G_1. Take now a maximum invariant subgroup G_2 of G_1 and proceed as before. The solution of the given equation depends by this method upon a chain of resolvents

$$\Phi_1 = 0, \quad \Phi_2 = 0, \ldots \Phi_\lambda = 0$$

corresponding respectively to

$$G_1, \quad G_2, \ldots G_\lambda = 1$$

which are the elements of a series of composition of G. Such a chain of resolvents is of especial importance as we shall now see.

28. Group of a rational resolvent. Isomorphism. Whichever of the above methods we employ to solve the given equation, the solution depends finally upon the solution of a chain of resolvents

$$\Psi_1 = 0, \quad \Psi_2 = 0, \ldots .$$

It is natural to apply Galois' methods to the solution of these. To do this the first requirement is to find their Galoisian Groups for their respective domains of rationality. These are obtained as follows. Suppose at a given moment the domain is R, and the group of the given equation is G. Let H, I, Φ, ϕ_1, ϕ_2, . . ϕ_r have the same significance as in §§22, 26. Denote the substitutions of I by 1, a, b, c, and let ρ be the index of I under G. We can arrange G in the array:

$$(B) \qquad \begin{array}{llll} 1 & a & b & \ldots \\ g_2 & ag_2 & bg_2 & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ g_\rho & ag_\rho & bg_\rho & \ldots \end{array}$$

Since $\phi_1, \ldots \phi_r$ are rational functions of $x_1, \ldots x_n$, let us apply to them a substitution of G; this will effect a substitution among the ϕ's. Obviously the substitutions in one and the same row in (B) produce the same substitution on the ϕ's; and no substitution in one row of (B) produces the same substitution among the ϕ's as a substitution in another row. For, since the substitutions in the same row produce the same substitution on the ϕ's we can reason on the first substitutions in each row. If now g_ι produces the same substitution on the ϕ's as g_κ, certainly g_κ^{-1} produces the reverse effect on the ϕ's from that of g_ι. Hence $g_\iota g_\kappa^{-1}$ leaves all the ϕ's unchanged; hence $g_\iota g_\kappa^{-1} = d$, a substitution of I; or $g_\iota = dg_\kappa$, *i.e.* g_ι is in the *same* row as g_κ.

There are thus exactly ρ substitutions of the ϕ's. Call them

$$J; \qquad \alpha, \beta, \gamma, \ldots$$

To every substitution of G corresponds one substitution of J but to one substitution of J correspond e substitutions of G, viz., all the substitutions on a certain line of (B).

If s, t be substitutions of G to which σ, τ correspond in J, then to st will correspond $\sigma\tau$. Evidently if s', t' be in the same rows respectively as s, t, then to $s't'$ will correspond also $\sigma\tau$. Obviously the substitutions J form a group.

Definition. If the substitutions of two groups $A = \{a_1, a_2, \ldots\}$ and $B = \{b_1, b_2, \ldots\}$ can be put in correspondence so that: 1° to one substitution of A, corresponds one of B, while to one of B correspond m of A; 2° if $b_\iota b_\kappa$ corresponds to $a_\iota a_\kappa$, when b_ι, b_κ correspond to a_ι, a_κ; then A, B are said to be isomorphic, and the isomorphism is in fact m to 1. Evidently to any subgroup of A corresponds a subgroup of B and conversely. In particular to an invariant subgroup of B will correspond an invariant subgroup of A.

From this definition follows that G, J have an e to 1 isomorphism.

We can prove now the

THEOREM: *The Galoisian group of $\Phi = 0$ for the domain R, is the group J.*

For, 1°. Every rational function $\psi(\phi_1, \phi_2, \ldots)$ unaltered by J lies in R. For, replacing the ϕ's by the x's, we have

$$\psi(\phi_1, \ldots \phi_r) = \chi(x_1, \ldots x_n).$$

As ψ is unaltered by J, χ is unaltered by G and hence lies in R.

2°. If ψ lies in R, it is unaltered by J. For if ψ lies in R, so does χ. But then χ is unaltered for G, hence ψ is unaltered for J.

Hence by §12, J is the group of $\Phi = 0$.

29. Group of a resolvent corresponding to a maximum invariant subgroup. Simple groups.

Definition. A group which contains no invariant subgroup besides 1, is called *simple*.

If the subgroup H of G used to form a resolvent $\Phi = 0$ is a maximum invariant subgroup, the group J of $\Phi = 0$ is simple. For if J had an invariant subgroup $K \neq 1$, G would have an invariant subgroup which would contain H.

If the group J of a resolvent $\Phi = 0$ is not simple the reasoning of the preceding paragraphs shows that its solution can be made to depend upon a chain of resolvents of simpler nature than $\Phi = 0$. If, however, J is simple this cannot be done. Thus resolvents which correspond to a series of composition are the simplest that can be chosen. Hence their theoretical importance; hence also the importance of the notion of a series of composition.

30. Cyclic equations. Factors of composition. The case when the index of an invariant subgroup H under G is a prime p, is of special interest. Such a group is obviously a *maximum* group, and the group J of the corresponding resolvent $\Phi = 0$ being of order p consists of the p powers of a cyclic substitution.

Definition. An equation whose group is cyclic is called a cyclic equation. Hence in the present case $\Phi = 0$ is a cyclic equation of prime degree, p.

Definition. Let $G, G_1, G_2, \ldots G_\lambda$, be a series of composition of G. Let f_κ be the index of G_κ under $G_{\kappa-1}$. Then $f_1, f_2, \ldots f_\lambda$ are called factors of composition of G.

Remark. We can show that however we decompose G into a series of composition, the factors of composition, aside from their order, are identical. They are an invariant of the group. We shall not make use of this fact, for the present. The example of §27 illustrates the invariance of these factors. In one case we get 2, 3; in the other 3, 2.

The above results may now be expressed in the

THEOREM. *The chain of resolvents corresponding to a series of composition whose factors of composition are all primes, is made up only of cyclic equations of prime degrees.*

Such equations can be solved algebraically, as we now show.

31. Solution of cyclic equations $\Phi(x) = 0$ of prime degree p.

Let R be a domain which, besides containing the coefficients of the given equation $\Phi(x) = 0$, contains an imaginary pth root of unity, ρ. For this

domain let the group G of $\Phi = 0$ be cyclic. Call the roots of $\Phi = 0$, $x_0, x_1, \ldots x_{p-1}$ and set $\gamma = (0, 1, \ldots p-1)$.

Then $$G = \{1, \gamma, \gamma^2, \ldots \gamma^{p-1}\}.$$

Consider now the rational functions:

$$\theta_h = x_0 + \rho^h x_1 + \cdots + \rho^{h(p-1)} x_{p-1}; \qquad h = 1, 2, \ldots p-1.$$

On applying γ they go over into $\rho^{-h}\theta$. Hence $\theta_h^p = \Theta_h$ are unchanged for γ and hence for G. They therefore are rationally known, and can thus be found (Remark §12, 1°). On extracting a pth root we get:

$$(a) \qquad x_0 + \rho^h x_1 + \cdots + \rho^{h(p-1)} x_{p-1} = \sqrt[p]{\Theta_h}; \qquad h = 1, 2, \ldots p-1.$$

To complete this system observe that the left hand side of

$$(b) \qquad x_0 + x_1 + \ldots + x_{p-1} = \sqrt[p]{\Theta_0}$$

is, aside from its sign, equal to the coefficient of x^{p-1} in $\Phi = 0$. To conform with the previous notation call this $\sqrt[p]{\Theta_0}$. To solve the system, (a), (b), observe that $\sum_{\kappa=0}^{p-1} \rho^{h\kappa} = 0$ for $h = 1, 2, \ldots p-1$ and $= p$ for $h = 0$. Hence to get x_κ multiply the equations (a) respectively by $\rho^{-h\kappa}$, $h = 1, 2, \ldots p-1$, and add the resulting equations to (b). We get, dividing by p,

$$x_\kappa = \frac{1}{p} \sum_{h=0}^{p-1} \rho^{-h\kappa} \sqrt[p]{\Theta_h} \qquad \kappa = 0, 1, 2, \ldots p-1.$$

The pth roots which enter here must be determined uniquely. To do this fix one of them say $\sqrt[p]{\Theta_1}$. The others are rational in this one, for

$$(x_0 + \rho^h x_1 + \cdots + \rho^{(p-1)h} x_{p-1})(x_0 + \rho\, x_1 + \cdots + \rho^{p-1} x_{p-1})^{p-h} = A_h$$

remains unaltered for γ and hence for G. Its value A_h can thus be expressed in known quantities (Remark §12, 1°). Hence

$$x_\kappa = \frac{1}{p\Theta_1} \sum \rho^{-h\kappa} A_h (\sqrt[p]{\Theta_1})^h.$$

Remark. The reasoning above applies to a cyclic equation of any degree q, if ρ be a primitive qth root of unity.

From this we have the

THEOREM: *Cyclic equations can be solved algebraically i. e. by extraction of roots from known quantities.*

This theorem together with that of §30 gives us a sufficient condition in order that a given equation can be solved algebraically.

THEOREM. *In order that an equation can be solved algebraically it is sufficient that its group admits a series of composition whose factors are all primes.*

We shall see in Part II that this condition is also necessary.

APPLICATION OF THE GENERAL THEORY TO THE SOLUTION OF BIQUADRATIC EQUATIONS.

32. General statement of method. The general biquadratic:

$$f(x) = x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = 0, \tag{1}$$

whose roots we denote by x_1, x_2, x_3, x_4, affords an excellent example to illustrate the methods of Galois' theory.

We suppose the coefficients to be indeterminate; the roots will then be independent variables. Thus equality between two rational functions takes place only when they are formally the same. As domain of rationality R, we take a domain containing the coefficients and such constants as we choose.

For R, the Galoisian group G of (1) is the symmetric group S_4 in x_1, x_2, x_3, x_4, § 15. All possible schemes for solving (1) are indicated on finding all the subgroups of G. Any subgroup H of G gives us an infinity of rational resolvents $\Phi = 0$, $\Psi = 0$, . . . corresponding to the infinity of rational functions $\phi, \psi, \ldots$. belonging to H. The roots $\phi, \psi, \ldots$ of these different resolvents corresponding to H are rational in one another, § 21. The solution of one of these, say $\Phi = 0$, and the adjunction of one or more of its roots reduces the group of (1) to a definite subgroup G_1 of G, § 25. With G_1 we can proceed as before. The solution of (1) can thus be varied in two ways 1° by taking different sets of subgroups to form our resolvents, 2° by taking different rational functions belonging to a given subgroup. The former offers a finite, the latter an infinite variety to choose from. All the solutions of the biquadratic equations, and their number is immense,* which have been proposed, must be reducible to this scheme. The Galoisian theory enables us, thus, to seize what is essential in each of these solutions and to see clearly their interrelations.

33. The subgroups of S_4. A simple train of reasoning permits us systematically to find all these. For our purpose the following groups suffice:

---

* *Cf.* L. Matthiessen. *Grundzüge der Antiken und Modernen Algebra.* Leipzig, 1878.

A_4; The alternate group of S_4:

1, (12)(34), (13)(24), (14)(23), (123), (124), (134), (234), (132), (142), (143), (243).

O; The octic group:

1, (1324), (13)(24), (1423), (12), (34), (12)(34), (14)(23).

A; The axial group:

1, (12)(34), (13)(24), (14)(23).

B; The semi-axial group:

1, (12)(34).

By actual trial we find that A_4 is an invariant subgroup of S_4. Further A is an invariant subgroup of A_4; and B is an invariant subgroup of A. We observe, moreover, that A is also invariant for S_4 since it embraces all the substitutions common to the octic group and its conjugates.

A series of composition of S_4 is thus

$$S_4 \quad A_4, \quad A, \quad B, \quad 1$$

whose factors of composition are

2, 3, 2, 2.

We give now three methods of solution of which the second and third are well known.

34. First solution (Series of composition). We form our first resolvent by taking a rational function belonging to the alternate group A_4. The simplest such function is the product of the differences of the roots:

$$\phi = (x_1 - x_2)\,(x_1 - x_3)\,(x_1 - x_4)\,(x_2 - x_3)\,(x_2 - x_4)\,(x_3 - x_4),$$

whose square is the discriminant of $f(x)$,

$$\Delta = \frac{1}{27}\,(4\,I_2^3 - I_3^2)$$

where I_2, I_3 are the quadratic and cubic invariants of f:

$$I_2 = a_2^2 - 3\,a_1\,a_3 + 12\,a_4,$$

$$I_3 = 27\,a_1^2\,a_4 + 27\,a_3^2 - 9\,a_1\,a_2\,a_3 - 72\,a_2\,a_4 + 2\,a_3.$$

Our first resolvent is thus,

$$\Phi = \phi^2 - \Delta = 0.$$

On adjoining $\phi = \sqrt{\Delta}$, our domain is $R'(R, \phi)$ for which the group of (1) is A_4.

Our next subgroup is the axial group A. A rational function belonging to this is $\psi = x_1 x_2 + x_3 x_4$. This gives the resolvent:

$$\Psi = \psi^3 - a_2 \psi^2 + (a_1 a_3 - 4 a_4)\psi - \{a_4(a_1^2 - 4 a_2) + a_3^2\} = 0.$$

The solution of this cubic gives ψ as a known explicit algebraic function of quantities in R. Adjoin ψ, giving the new domain $R''(R, \phi, \psi)$. For this domain our group is A.

The next subgroup is the semi-axial group B. To this belongs

$$\chi = (x_1 + x_2) - (x_3 + x_4)$$

root of the quadratic

$$X = \chi^2 - (4\psi + a_1^2 - 4 a_2) = 0.$$

Solving this, gives χ as an algebraic function of known quantities. Adjoining it our domain becomes $R'''(R, \phi, \psi, \chi)$ for which the Galoisian group is B.

The next group is the identical group 1, to which x_1 belongs. Its corresponding resolvent is

$$x^3 + \tfrac{1}{2}(a_1 - \chi)x + \tfrac{1}{2}\left(\psi + \frac{2a_3 - a_1\psi}{\chi}\right) = 0.$$

Solving this, we find x_1, whose adjunction gives a domain $R^{IV}(R, \phi, \psi, \chi, x_1)$ for which the group is 1 and in which all the roots must lie. To show this we notice that x_1 obviously lies in R^{IV}. That x_2 is there, we see by observing that

$$x_1 + x_2 = -\tfrac{1}{2}(a_1 - \chi), \quad \therefore \quad x_2 = -x_1 - \tfrac{1}{2}a_1 + \tfrac{1}{2}\chi.$$

Turn now to x_3, x_4. The cubic $\Psi = 0$ is cyclic; hence its roots, ψ', ψ'' are rational in ψ. Hence

$$(x_1 - x_2)(x_3 - x_4) = \psi' - \psi'' = \alpha$$

must lie in R^{IV} as we actually show in a moment.

Now we have just seen that $x_1 - x_2 = \beta$ and $x_1 + x_2 = \gamma$ lie in R^{IV}. Hence $\beta(x_3 - x_4) = \alpha$, together with $x_1 + x_2 + x_3 + x_4 = \gamma + x_3 + x_4 = -a_1$ give x_3, x_4, which therefore lie in R^{IV}.

To calculate α we observe that

$$(1) \qquad \alpha = \psi' - \psi'' = \frac{(\psi - \psi')(\psi - \psi'')(\psi' - \psi'')}{(\psi - \psi')(\psi - \psi'')}.$$

But the numerator here is the square root of the discriminant of $\Psi = 0$ and this is the same as the discriminant of (1). The denominator is obviously $\Psi'(\psi)$, the accent indicating differentiation. Hence $a = \sqrt{\Delta}/\Psi'(\psi)$, a quantity obviously in R^{IV}.

35. Second solution (Lagrange). To build the first resolvent Lagrange starts with the octic group O. As a function belonging to this group he uses:*

$$\phi = \{(x_1 + x_2) - (x_3 + x_4)\}^2$$

whose conjugates are $\phi_1 = \{(x_1 + x_3) - (x_2 + x_4)\}^2$, $\phi_2 = \{(x_1 + x_4) - (x_3 + x_2)\}^2$, giving the resolvent:

$$\Phi = \phi^3 - (3a_1^2 - 8a_2)\,\phi^2 + (3a_1^4 - 16a_1^2 a_2 + 16a_2^2 + 16a_1 a_3 - 64a_4)\,\phi - (a_1^3 - 4a_1 a_2 + 8a_3)^2 = 0.$$

Solve this and adjoin all its roots, giving the domain $R_1(R, \phi, \phi_1, \phi_2)$. For this the group of (1) is the axial group A, §34.

Take as next subgroup, the semi-axial group B. As a function belonging to this Lagrange takes

$$\psi = (x_1 + x_2) - (x_3 + x_4),$$

which gives obviously the resolvent

$$\Psi = \psi^2 - \phi = 0.$$

Adjoining ψ, our domain becomes $R_2(R, \phi, \phi_1, \phi_2, \psi)$, for which the group is B.

The next and last group is 1. To this belongs

$$\chi = (x_1 + x_3) - (x_2 + x_4)$$

which gives the resolvent

$$X = \chi^2 - \phi = 0.$$

The adjunction of χ reduces our group to 1, and now all the roots are in the resulting domain, $R_4(R, \phi_1, \phi_2, \phi_3, \psi, \chi)$; for,

$$(a) \qquad \begin{aligned} x_1 + x_2 - x_3 - x_4 &= \psi = \pm\sqrt{\phi}, \\ x_1 + x_3 - x_2 - x_4 &= \chi = \pm\sqrt{\phi_1}, \\ x_1 + x_4 - x_3 - x_2 &= \pm\sqrt{\phi_2}, \\ x_1 + x_2 + x_3 + x_4 &= -a_1, \end{aligned}$$

*Observe that the letters ϕ, ψ, χ do not represent the same functions in the different solutions.

which give

$$x_\kappa = \tfrac{1}{4}\,(-a \pm \sqrt{\phi} \pm \sqrt{\phi_1} \pm \sqrt{\phi_2}) \qquad (\kappa = 1, 2, 3, 4.)$$

Here we choose at will the signs of $\sqrt{\phi}$, $\sqrt{\phi_1}$. The sign of $\sqrt{\phi_2}$ is then determined for

$$(b) \qquad \sqrt{\phi}\cdot\sqrt{\phi_1}\cdot\sqrt{\phi_2} = 4\,a_1 a_2 - a_1^3 - 8\,a_3.$$

36. Third solution (Invariants). The principles being here the same as in §34, §35 we indicate the solution briefly as follows: The subgroups employed are the same as in the first solution §34, viz., the alternate, the axial, the semiaxial and the identical group; but the functions used to build resolvents corresponding to the second and fourth groups are different.

A_4 $\qquad \phi = \prod_{\iota,\kappa} (x_\iota - x_\kappa)\,; \qquad \Phi = \phi^2 - \Delta = 0.$

A ; $\psi = (x_1 - x_2)\,(x_3 - x_4)\,; \quad \Psi = \psi^3 - I_2\,\psi + \sqrt{\Delta} = 0\,;$ Conjugate roots $\psi_1 = (x_1 - x_3)(x_4 - x_2)$ and $\psi_2 = (x_1 - x_4)\,(x_2 - x_3)$.

B; $\chi = (x_1 + x_2) - (x_3 + x_4)\,; \quad \mathrm{X} = \chi^2 - \tfrac{1}{3}\,(3a_1^2 - 8\,a_2 - 4\,\psi_1 + 4\psi_2) = 0.$

1 ; $\xi = (x_1 + x_3) - (x_2 + x_4)\,; \quad \Xi = \xi^2 - \tfrac{1}{3}\,(a_1^2 - 8a_2 + 4\,\psi - 4\psi_2) = 0.$

Here we determine x_1, x_2, x_3, x_4 by a set of equations similar to (a) §35 using the relation corresponding to (b). To do this we need ψ_1, ψ_2. We proceed as in the corresponding case of §34. To this end we need only the numerator of (1) §34, viz.: $(\psi - \psi_1)(\psi - \psi_2)(\psi_1 - \psi_2)$. This, we observed, is the square root of the discriminant of $\Psi = 0$ which here is I_3^2. Taking the proper sign, on extracting the square root we have

$$(\psi - \psi_1)(\psi - \psi_2)(\psi_1 - \psi_2) = I_3.$$

NEW HAVEN, CONN., FEBRUARY, 1900.

EVALUATION OF A DEFINITE INTEGRAL.*

By A. Pell.

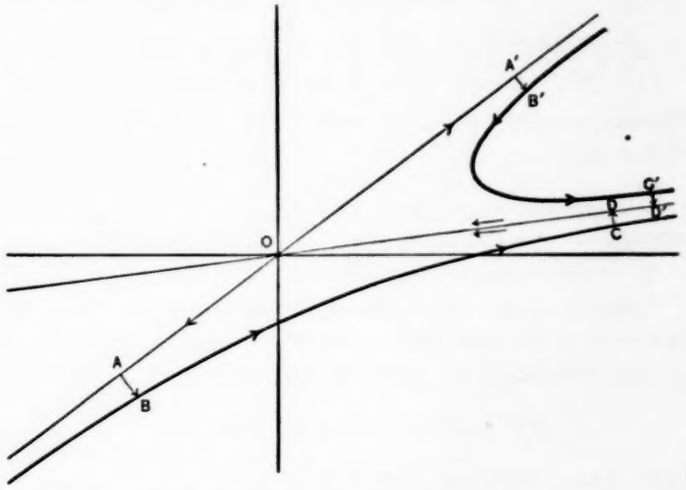
In his book on definite integrals, Bierens de Haan gives the following formulæ:

$$\int_0^\infty e^{-(px^2+q/x^2)} \begin{matrix}\sin\\ \cos\end{matrix}\left\{ rx^2+\frac{s}{x^2}\right\} dx=\frac{\sqrt{\pi}}{2a}\, e^{-2ab\cos(\alpha+\beta)} \begin{matrix}\sin\\ \cos\end{matrix}\left\{ 2ab\sin(\alpha+\beta)+\alpha\right\},$$

where:

$$a^4=p^2+r^2, \quad b^4=q^2+s^2, \quad \alpha=\tfrac{1}{2}\tan^{-1}\frac{r}{p}, \quad \beta=\tfrac{1}{2}\tan^{-1}\frac{s}{q}.$$

For the proof reference is made to a book by Helmling,† which seems to be



quite inaccessible, as it is to be found neither in the Göttingen nor in the Berlin university library.

We will establish the above formulæ on the supposition that $p>0$, $q>0$,‡ by making use of the fact that the integral of e^{-z^2} around any closed contour

---

*This paper was read before the Chicago section of the American Mathematical Society at the Meeting of Dec. 28, 1899.

† *Transformation und Ausmittelung bestimmter Integrale*, 1854.

‡ If either p or q is negative the above integral has no meaning. We will not consider cases in which p or q is zero.

in the complex z-plane is zero. The contour we shall use is the one marked in the figure $OABCDO$, and consists of an arc of a hyperbola BC, of portions OA and DO of its asymptotes, and of the arcs AB and CD of two circles with centre at O. Letting $z = X + iY$ we will represent our hyperbola by the two equations:

$$X = Px - \frac{Q}{x}, \qquad Y = Rx - \frac{S}{x},$$

where x is a parameter, and P, Q are both positive. Eliminating x between these two equations, we get as the equation of the hyperbola:

$$SRX^2 + PQY^2 - (PS + RQ)XY - (PS - RQ)^2 = 0.$$

Integrating around the contour we have:

$$\int_{OABCDO} e^{-z^2} dz = 0 = \int_{OA} + \int_{AB} + \int_{BC} + \int_{CD} + \int_{DO}.$$

When the radii of the arcs AB and CD are increased indefinitely:*

$$\lim \int_{CD} = \lim \int_{AB} = 0, \qquad \text{and} \qquad \lim \int_{OA} = \lim \int_{DO} = -\frac{\sqrt{\pi}}{2},$$

provided that the slopes of the asymptotes are numerically less than 1; *i. e.* provided $S^2 < Q^2$ and $R^2 < P^2$. We will henceforth assume that these inequalities hold, so that we have:

$$\lim \int_{BC} e^{-z^2} dz = \sqrt{\pi}.$$

When z varies along BC, the parameter x varies from 0 to ∞, hence substituting and carrying out the indicated operations, we find:

$$\int_0^\infty e^{-[(P^2 - R^2)x^2 + (Q^2 - S^2)/x^2]} \left\{ \cos 2\left[RPx^2 + \frac{SQ}{x^2} - (RQ + SP) \right] - i \sin 2 \left[RPx^2 + \frac{SQ}{x^2} - (RQ + SP) \right] \right\} \left(P + \frac{Q}{x^2} + i\left(R + \frac{S}{x^2}\right) \right) dx = e^{-2(PQ - RS)} \sqrt{\pi}.$$

Separating real and imaginary parts of this equation we shall have:

$$\int_0^\infty e^{-[(P^2 - R^2)x^2 + (Q^2 - S^2)/x^2]} \left[\left(P + \frac{Q}{x^2}\right) \cos 2 \left\{ RPx^2 + \frac{SQ}{x^2} - (RQ + SP) \right\} + \left(R + \frac{S}{x^2}\right) \sin 2 \left\{ RPx^2 + \frac{SQ}{x^2} - (RQ + SP) \right\} \right] dx = e^{-2(PQ - RS)} \cdot \sqrt{\pi},$$

* Picard, *Traité d'Analyse*, Vol. II, p. 159.

$$\int_0^\infty e^{-[(P^2-R^2)x^2+(Q^2-S^2)/x^2]}\Big[(P+\frac{Q}{x^2})\sin 2\Big\{RPx^2+\frac{SQ}{x^2}-(RQ+SP)\Big\}$$
$$-(R+\frac{S}{x^2})\cos 2\Big\{RPx^2+\frac{SQ}{x^2}-(RQ+SP)\Big\}\Big]dx=0.$$

Integrating the same function along the conjugate hyperbola:

$$X=Px+\frac{Q}{x},\qquad Y=Rx+\frac{S}{x},$$

we find two more equations:

$$\int_0^\infty e^{-[(P^2-R^2)x^2+(Q^2-S^2)/x^2]}\Big[(P-\frac{Q}{x^2})\begin{matrix}\cos\\ \sin\end{matrix}2\Big\{RPx^2+\frac{SQ}{x^2}+(RQ+SP)\Big\}$$
$$\pm(R-\frac{S}{x^2})\begin{matrix}\sin\\ \cos\end{matrix}2\Big\{RPx^2+\frac{SQ}{x^2}+(RQ+SP)\Big\}\Big]dx=0.$$

Let α and β be the angles which the asymptotes make with the axis of reals. We have:

$$\tan\alpha=\frac{R}{P},\quad \tan\beta=\frac{S}{Q}.$$

Let also:

$$P^2-R^2=p,\quad Q^2-S^2=q,\quad 2PR=r,\quad 2QS=s,\quad \sqrt{p^2+r^2}=a^2,\quad \sqrt{q^2+s^2}=b^2.$$

We then have:

$$\tan 2\alpha=\frac{r}{p},\qquad \tan 2\beta=\frac{s}{q},$$
$$P=a\cos\alpha,\quad R=a\sin\alpha,\quad Q=b\cos\beta,\quad S=b\sin\beta,$$

and the only conditions to which p, q, r, s need be subjected are evidently:

$$p>0,\qquad q>0.$$

By substituting these values of P, Q, R, S in the four integrals obtained above and combining them we get:

$$\int_0^\infty e^{-(px^2+q/x^2)}\Big\{\cos\alpha\cdot\begin{matrix}\cos\\ \sin\end{matrix}\Big(rx^2+\frac{s}{x^2}\Big)\pm\sin\alpha\cdot\begin{matrix}\sin\\ \cos\end{matrix}\Big(rx^2+\frac{s}{x^2}\Big)\Big\}dx$$
$$=\frac{\sqrt{\pi}}{2a}e^{-2ab\cos(\alpha+\beta)}\cdot\begin{matrix}\cos\\ \sin\end{matrix}\Big\{2ab\sin(\alpha+\beta)\Big\},$$

from which the formulæ given at the beginning of this paper follow.

UNIVERSITY OF SOUTH DAKOTA, DECEMBER, 1899.

TWO NON-ISOMORPHIC SIMPLE GROUPS OF THE SAME ORDER 20,160.*

By Ida May Schottenfels.

1. Introduction. It has never been proved that two simple groups of the same order are necessarily holoedrically isomorphic;† nor has any example been heretofore noticed of two simple groups of the same order which are not holoedrically isomorphic, or abstractly identical.

Dickson‡ has proved that all k-ary linear fractional substitution groups in the Galois Field $[p^n]$§ (p is a prime, n is a positive integer) with determinant unity, are simple; and, among others, he enumerates the ternary linear fractional substitution group of order $8!/2$ in the Galois Field $[2^2]$.

Since no element of period fifteen and no element of period six could be found in this group, the suspicion arose that this group was not holoedrically isomorphic to the alternating group of degree eight,‖ a simple group of the same order, containing substitutions of periods fifteen and six.

At Professor Moore's suggestion the investigation is made as to whether or not these two groups are holoedrically isomorphic, and it is found that *no such isomorphism exists.* The present paper furnishes the first direct proof of this theorem, which has recently been corroborated by Mr. Dickson, whose proof will shortly be published.

2. The Ternary Group. The first group with which we have to deal is the ternary fractional group in the Galois Field $[2^2]$. Without pre-

---

*This paper was read before the Seminar on Group Theory, held by Professor Moore, March, 1898; and later before the Chicago Mathematical Club held January 21, 1899, at the Univ. of Chicago.

†Holoedric isomorphism is the only isomorphism that can exist between two simple groups.

‡Dickson: Annals of Mathematics, 1st Ser. Vol. 11, 1897, pp. 175-178.

§The expression Galois Field is perhaps not yet in general use. The notion is due to Galois and is fully developed by Serret: *Algèbre supérieure*, Vol. 2, pp. 122-189. The theory in its abstract form is developed by Moore: *Proceedings of the Congress of Mathematics of 1893 at Chicago*, pp. 208-242, 1896, also in the *Bull. of the N. Y. Math. Soc.*, Vol. 3, pp. 73-78, 1894, and by Borel et Drach: *Théorie des Nombres et Algèbre supérieure* 1895, pp. 42-50, 58-62, 343-350.

‖Jordan: *Traité des Substitutions*, pp. 380-382, and Moore: *Math. Ann.* Vol. 51, pp. 417-444, have shown that the quaternary linear homogeneous substitution group of order $8!/2$ in the Galois Field $[2^1]$, and the alternating group of degree eight, both of which are simple, *are* holoedrically isomorphic.

supposing any knowledge of the theory of the Galois Field, this group may be defined as follows:

It is a group of so-called *Fractional Matrices*:

$$\left(\begin{array}{ccc} \xi_{11} & \xi_{12} & \xi_{13} \\ \xi_{21} & \xi_{22} & \xi_{23} \\ \xi_{31} & \xi_{32} & \xi_{33} \end{array}\right) = (\underline{\underline{\xi_{ij}}}). \qquad (i, j = 1, 2, 3)$$

The elements of these matrices are quantities of the form $a + b\rho$ where ρ is a complex cube root of unity and a and b are rational integers. Two such matrices $(\underline{\underline{\xi_{ij}}})$, $(\underline{\underline{\xi_{ij}}})$ are defined as equal if, and only if, there exists a quantity μ of the form $a + b\rho$ (a, b, ρ having the same meaning as above) such that:*

$$\mu\, \xi_{ij} \equiv \xi'_{ij} \pmod 2.$$

We consider only those matrices whose determinant is congruent to 1 (mod. 2). *These matrices form a group of order* $8!/2$, the ternary group in question, *provided that we take as our law of composition the general law of matrices.*

$$A = (\underline{\underline{a_{ij}}}), \quad B = (\underline{\underline{b_{jk}}}), \quad C = (\underline{\underline{c_{ik}}}), \quad AB = C, \quad \sum_{j=1,2,3} a_{ij} b_{jk} = c_{ik}.$$

The identity matrix is

$$I = \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right).$$

We make use of two other special matrices of this group,†

$$\left(\begin{array}{ccc} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}\right) = B, \qquad \left(\begin{array}{ccc} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \rho & 0 \end{array}\right) = C.$$

The matrices B, C, and $F = CB^6$ satisfy the following system Σ of relations:

$$\Sigma(B, C, F): \quad \left\{ \begin{array}{l} B^7 = C^7 = (B^2C)^5 = (BC)^4 = (CB)^3 = I \\ F = CB^6,\ F^2 = I,\ C = FB \end{array} \right\}.$$

* A congruence $a + b\rho \equiv a' + b'\rho$, when a, b, a', b' are rational integers and ρ a complex cube root of unity, is equivalent to the two congruences $a \equiv a'$, $b \equiv b'$.

† These are special cases of a type of generator employed by Moore, *Math. Ann.*, Vol. 51, p. 436.

3. Comparison of the Ternary and Alternating Groups. We must seek to find, in the most general way, in the alternating group $G^8_{8!/2}$, substitutions b, c, and $f = cb^6$ satisfying the system Σ of relations,

$$\Sigma(b, c, f): \quad \left\{ \begin{array}{l} b^7 = c^7 = (b^2c)^5 = (bc)^4 = (cb^6)^2 = i \\ f = cb^6,\ f^2 = i,\ c = fb \end{array} \right\};$$

and if the ternary group above described be holoedrically isomorphic to the alternating, the alternating *must contain* substitutions b, c, and $f = cb^6$ satisfying the system Σ of relations, when i is the identity substitution of the group.

The alternating group of degree eight is well known, and its substitutions of period seven and of period two can be listed, and the following method of proof will suggest itself.

For b choose any one of the substitutions of period seven, for f any one of period two, and if the product $fb = c$ is of period seven make further trial of b^2c; should this be of period five, try finally the product bc and should this fail to be of period four, reject this f and assume for trial another f, say f' and go through the same process with f', b. Continue in this way until the f's are exhausted, and reject the assumed b. Starting with another b, say b', continue the same process. Finally a solution is found or else the b's must be exhausted. Owing to the very large number of f's and b's, this method is not feasible. In the following a comparatively short method of proof is exhibited.

SYNOPSIS OF THE PROOF.

§4. One substitution only of period seven is necessary for the investigation and the choice is made of $b' = (1\,2\,3\,4\,5\,6\,7)$.

§5. Only forty-five substitutions of period two *distinct with respect to transformation by powers of* $b' = (1\,2\,3\,4\,5\,6\,7)$ are needed in the investigation.

§6. These forty-five substitutions are discovered and listed in the table, page 152.

§7. The table shows wherein these substitutions fail to obey the system Σ of relations and definitive conclusions are drawn from these facts.

PROOF.

4. The most general substitution of period seven in the alternating

group is: $b = (l_1 l_2 l_3 l_4 l_5 l_6 l_7)$ where $l_1 l_2 l_3 l_4 l_5 l_6 l_7$ are seven of the eight numbers 1, 2, 3, 4, 5, 6, 7, 8 taken in any order. The transformed substitution of a substitution π by another substitution s, we denote by π_s so that $\pi_s = s^{-1} \pi s$.

Assume that there exists in the alternating group $G^8_{8!/2}$ one set of substitutions (b, c, f) satisfying the system of relations $\Sigma(b, c, f)$. By transforming by any substitution t of the symmetric group we have the set (b, c, f) transformed into (b_t, c_t, f_t), and these also are substitutions of the alternating group, since it is invariant under transformation by the symmetric group. Further, the transformed set also satisfy the system of relations $\Sigma(b_t, c_t, f_t)$, as shall presently be proved. Finally, the substitution t can be so chosen that b is transformed into any desired substitution b' of period seven, *e. g.* into the particular substitution $b' = (1\,2\,3\,4\,5\,6\,7)$. For, if we have, as above, $b = (l_1 l_2 l_3 l_4 l_5 l_6 l_7)$, then, using the two-rowed notation, we may take as t the substitution

$$t = \begin{pmatrix} l_1 & l_2 & l_3 & l_4 & l_5 & l_6 & l_7 & l_8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix},$$

whence, evidently, we have the desired result:

$$t^{-1} b\, t = b_t = (1\,2\,3\,4\,5\,6\,7) = b'.$$

The proof of the second statement is the following: Given two products as in the Σ system of relations, $\Pi_1(b, c, f) = \Pi_2(b, c, f)$, then by transforming by t we have $\Pi_1(b, c, f)_t = \Pi_2(b, c, f)_t$ since this is a group process. Applying the theorem:

The transform of a product is the product of the transforms of the individual factors, and making use of the notation $(b_t, c_t, f_t), = (b', c', f')$, we have

$$\Pi_1(b', c', f') = \Pi_2(b', c', f').$$

From the elements of period seven, $b' = (1\,2\,3\,4\,5\,6\,7)$ is chosen for the remainder of this discussion.

5. A system of substitutions s' exists, such that

$b'_{s'} = b' = (1\,2\,3\,4\,5\,6\,7) = (i+1, i+2, \ldots i+7)$ modulo 7, $(i = 0, 1, \ldots 6)$

i. e. the transformers s' leave b' invariant. The system of substitutions s' are powers of b'; for, using the two-rowed notation for the substitution s',

$$s' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ a_0 & a_0+1 & a_0+2 & a_0+3 & a_0+4 & a_0+5 & a_0+6 \end{pmatrix} = b'^{a_0 s^{-1}} \text{ (modulo 7)}.$$

This fact together with the relation, $c = fb$, reduces the work seven-fold

$$(b', c) f_{b^\mu} = (b', c', f') \text{ where } c' = f' b'.$$

Hence f' alone requires investigation, and but one f' from each of the systems of seven, resulting from transformation by powers of $b', b'_{b''}$.

6. A detailed study is now made of the substitutions f of the alternating group, where $f^2 = i$. These separate into two divisions (see table page 152). Division I consists of 15 products of four independent transpositions, distinct with respect to transformation by b'', which separate into 5 classes of 3 each. Division II consists of 30 products of two independent transpositions distinct with respect to transformation by b'', which separate into two sets, Set I, Set II, each containing 15 types. The 15 types of Set II separate into 5 classes of 3 each. These forty-five types have been so arranged in the table that the analytical proof of their distinctness with respect to transformations by powers of b'' follows very readily.

In Set II, Division II, the 3 substitutions of each of the five classes have the same residual numbers. Aside from 8, the omission of which characterizes them all, the residuals of the five classes respectively are the following:

1 2 3	(156),	4 5 6	(127),	7 8 9	(134),	10 11 12	(146),	13 14 15	(145).

A very neat graphical proof of the distinctness of these 5 classes may be made by considering these residuals as the vertices of triangles at the corners of a regular 7-gon, which triangles have, under cyclic permutation of the 7-gon into itself, 7 distinct positions; and by a discussion of the cyclic intervals into which each 7-gon is divided by its respective triangle.

7. The table on the next page shows that no one of the $15 + 30$ f's satisfies the system Σ of relations. We have then proved that in the alternating group there exists no solution (b, c, f) of the system Σ of relations $\Sigma(b, c, f)$.

There exists a totality of elements, BC-products in our ternary group, which have no corresponding elements in the alternating group.

Hence we have here an example of two simple groups of the same order, which are not holoedrically isomorphic, and so an example of two simple abstract groups of the same order which are not identical.

Table of the 45 f's and of their relation to the System Σ.**

DIVISION I.		DIVISION II.			
SET I.		SET I.		SET II.	
1	(81) (23) (45) (67)*	1	(81) (23)‡	1	(23) (74)*
2	(81) (23) (46) (57)‡	2	(81) (24)*	2	(24) (73)‡
3	(81) (23) (47) (56)*	3	(81) (34)‡	3	(34) (27)*
4	(81) (24) (35) (67)‡	4	(81) (45)‡	4	(45) (36)*
5	(81) (24) (36) (57)*	5	(81) (46)*	5	(46) (35)‡
6	(81) (24) (37) (56)‡	6	(81) (56)‡	6	(65) (34)*
7	(81) (25) (34) (67)*	7	(81) (76)‡	7	(76) (25)*
8	(81) (25) (36) (47)*	8	(81) (72)*	8	(27) (65)*
9	(81) (25) (37) (64)*	9	(81) (26)*	9	(26) (57)‡
10	(81) (26) (34) (75)‡	10	(81) (35)*	10	(35) (27)*
11	(81) (26) (35) (47)*	11	(81) (37)*	11	(37) (25)†
12	(81) (26) (37) (54)‡	12	(81) (57)*	12	(57) (23)*
13	(81) (27) (34) (65)*	13	(81) (25)*	13	(23) (76)*
14	(81) (27) (35) (46)*	14	(81) (36)*	14	(26) (73)†
15	(81) (27) (36) (54)*	15	(81) (47)*	15	(27) (36)*

**In the table the inequalities

	$(fb)^7 \neq i$	$(b^3c)^3 \neq i$	$(bc)^4 \neq i$
are denoted respectively by the marks	*	‡	†.

CHICAGO, JANUARY, 1900.

CONTENTS.

	PAGE
Rational Triangles. By Mr. Derrick N. Lehmer,	97
Two Elementary Geometrical Applications of Determinants. By Professor H. S. White,	103
On the Volume of a Polyhedron. By Professor H. B. Newson,	108
A Graphical Method of deducing the Criteria for the nature of the Roots of Cubic and Quartic Equations. By Professor R. E. Gaines,	111
Galois' Theory of Algebraic Equations. By Professor James Pierpont,	113
Evaluation of a Definite Integral. By Professor A. Pell,	144
Two Non-Isomorphic Simple Groups of the same Order 20,160. By Miss Ida May Schottenfels,	147

ANNALS OF MATHEMATICS.

Published in October, January, April, and July, under the auspices of Harvard University, Cambridge, Mass.

Terms of subscription: $2 a volume (four numbers), in advance. Single numbers seventy-five cents. All drafts and money orders should be made payable to Harvard University. Address: *The Annals of Mathematics*, 2 University Hall, Cambridge, Mass.

Printed by The Salem Press Co., Salem, Mass.